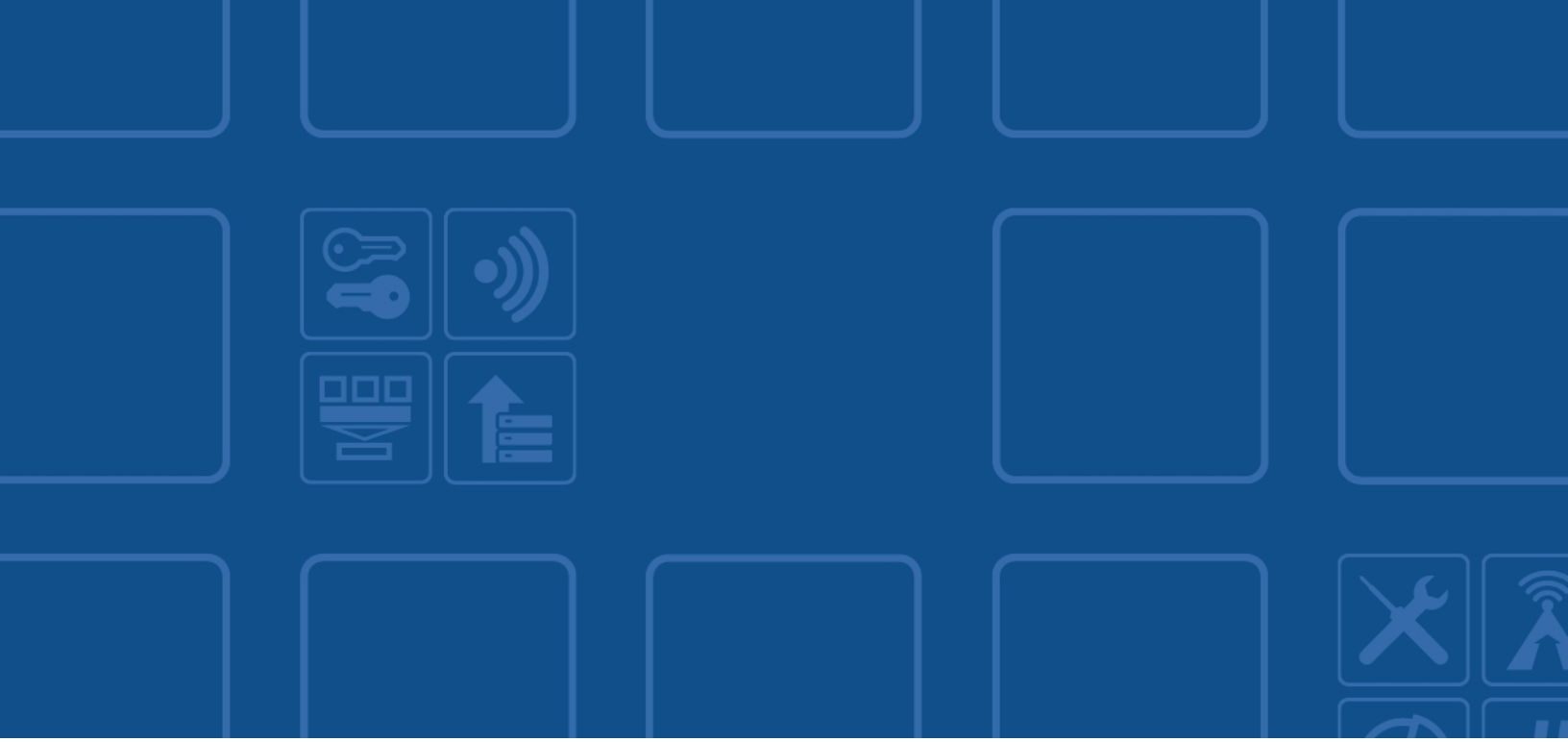
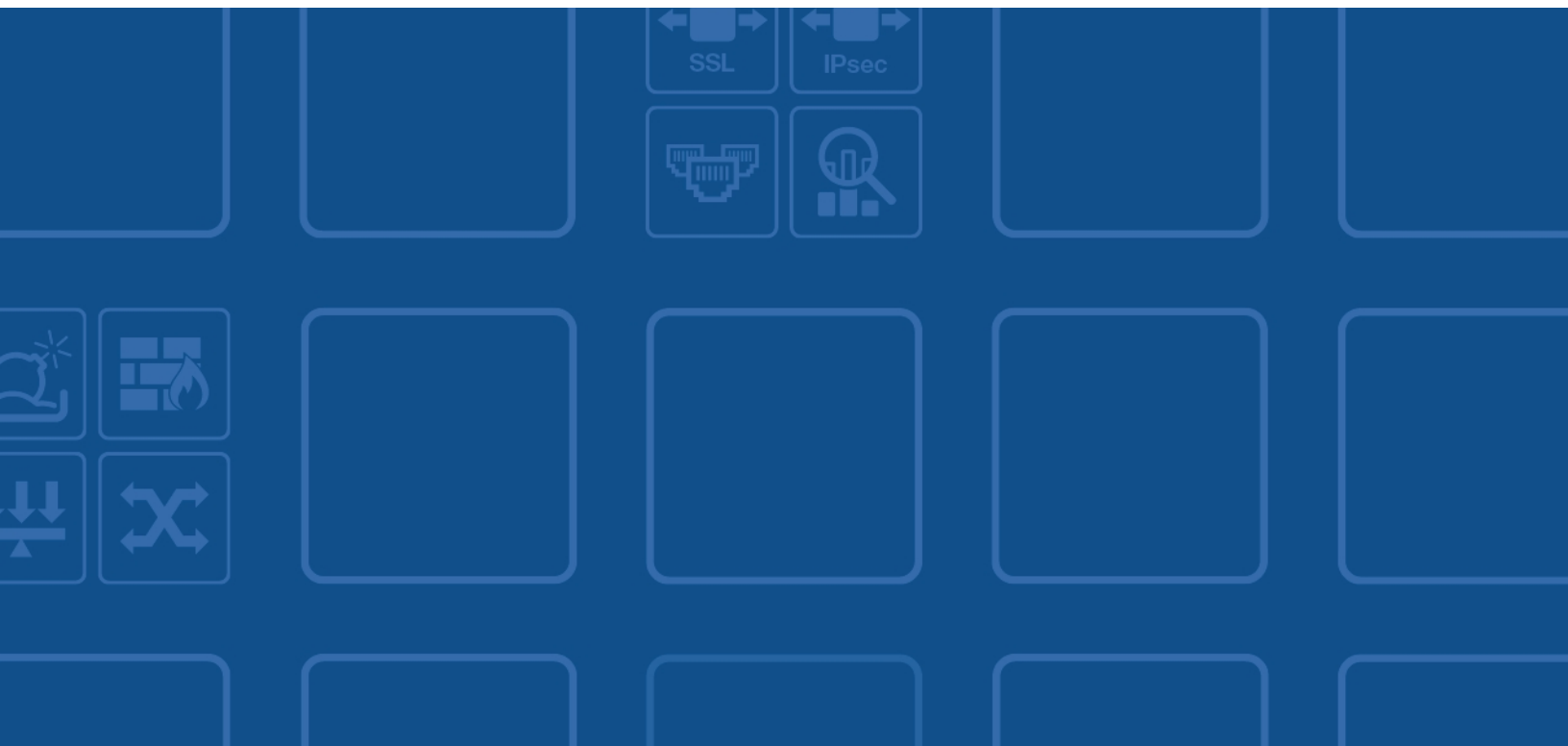


FORTINET
High Performance Network Security

FortiGate Connector for Cisco ACI - Administration Guide

Version 1.3



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, February 16, 2017

FortiConnector for Cisco ACI v.1.3 - Administration Guide

01-540-371313-20160505

TABLE OF CONTENTS

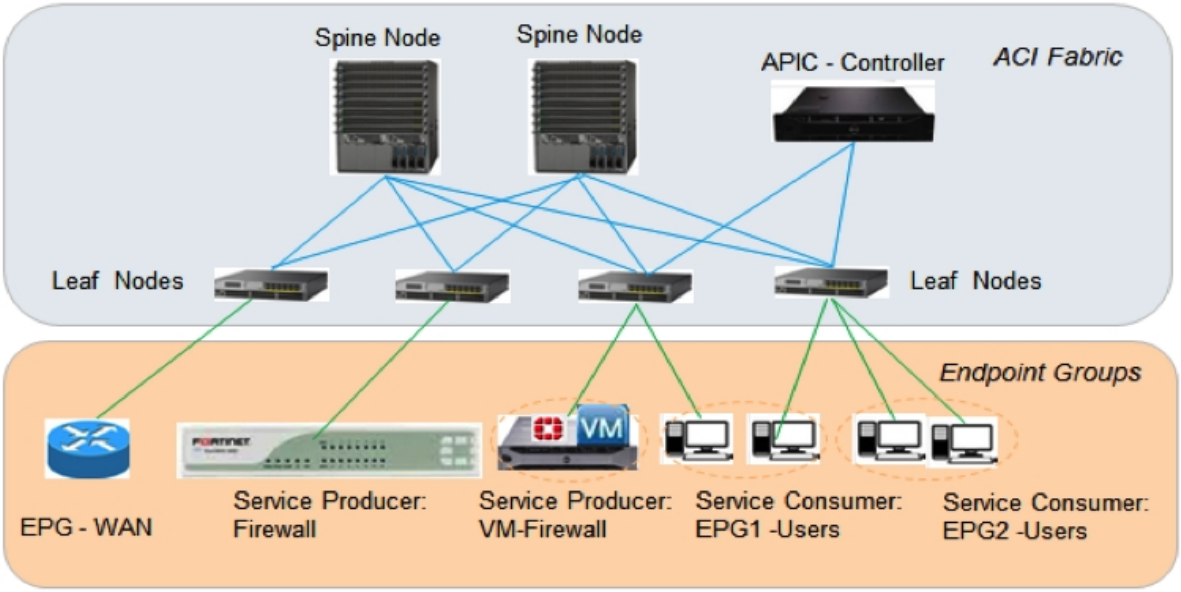
Change Log

Date	Change Description
2016-08-26	Initial Release of version 1.3

Overview

FortiGate Connector for Cisco ACI (Application Centric Infrastructure) is the Fortinet solution to provide seamless integration between Fortinet Firewall (Fortigate) deployments and the Cisco APIC (Application Policy Infrastructure Controller). This integration allows customers to perform single point of FortiGate configuration and Management operation through Cisco APIC.

While the FortiGate series of firewalls enable superb firewall services, in a data center environment, the insertion, configuration, and management of network services such as firewall can be quite complex and potentially error-prone tasks. One solution for such data center problems is Cisco's ACI. Cisco's ACI is a policy-based framework with integration of software and hardware in the underlying leaf-spine fabric. In Cisco ACI, the APIC is a tool used to automate service insertion and provisioning into the fabric of the network environment. Network service appliances, both physical and virtual, can be attached to ACI fabric's leaf node through APIC. Traffic demanding certain network services is steered by APIC-managed policies to the appropriate resources. The FortiGate Connector allows FortiGates to be included amongst the list of resources that traffic can be directed to.



Licensing

FortiGate Connector for Cisco ACI is free of charge for Fortinet customers. You need to make sure that you register your FortiGate with FortiCare on support.fortinet.com.

Terms and concepts

FortiGate VDOMs

VDOM or Virtual Domain refers to a discretely administered segment on a FortiGate firewall. A FortiGate firewall that is not segmented and where a single administrator can access all of the firewall is operating in the “root” VDOM. However, it is possible to segment the FortiGate so that different administrators can access different areas of the FortiGate. Credentials for VDOM X will allow access to the resources and settings of VDOM A but no other. There will also be global resources and settings that will require credentials to the root VDOM. When setting up connectivity between Cisco APIC and the FortiGates it will be important to know which VDOMs control the needed resources.

FortiOS RESTful API

REST (sometimes spelled ReST) stands for Representational State Transfer. It is a software architectural style for the WWW. REST systems typically communication over HTTP, using HTTP verbs or commands to retrieve and send information to remote servers.

A good resource for the finer details of Fortinet’s implementation of ReST can be found at http://docs.fortinet.com/uploaded/files/1276/FortiAuthenticator_REST_API_Solution_Guide.pdf

North/South and East/West Traffic

The cardinal compass direction terms to describe traffic flow are used to differentiate between traffic within the cloud or data center and traffic going in and out of the cloud or data center.

- North/South - traffic either heading into or out of a cloud or data center.
- East/West - traffic that is between nodes inside the same cloud or data center.

Features

There are a number of features associated with firewalls in general and FortiGate firewalls in particular. This section should explain which of these features are available through the FortiGate Connector and which are not.

Supported Features

The FortiGate Connector for Cisco ACI supports the following functions:

Baseline features from v.1.0 to v.1.1

- Cisco ACI service insertion - software package for FortiGate device deployed to Cisco APIC, containing FortiGate models, function description, version, credentials, as a L4-L7 service.
- Enable tenant configuration to add/modify/delete L4-L7 device of FortiGate firewall service.
- Enable FortiGate deployment as both physical and virtual device (FortiGate chassis & VM).
- Support both transparent (GoThrough) and L3 (GoTo) device mode .
- Automatically create VDOM (context). One VDOM per logical device under a tenant.
- Enable FortiGate specific interface configuration: physical interface and port channel.
- Support IP address configuration on Layer 3 interfaces.
- Support subnet and service object configuration.
- Enable FortiGate firewall device to connect to endpoint groups (EPGs).
- Support IPv4 policies: match, action, network operations & security features' selection.
- Support NAT.
- Enable service graph to add/modify/delete FortiGate firewall service node
- Multiple interfaces can be added in the same device
- Single logical port can be shared in the same EPG for multiple service graphs
- Single VDOM can be used in multiple service graphs

Additional features added in v1.2

- High Availability (Active-Standby Mode)
- OSPF based routing configuration in the L3 (GoTo) mode
- Support for logging and error reporting of Fortigate as a L4-L7 device
- Automatically create VDOM based on APIC virtual device ID
- Policy enable/disable support
- Enable/Disable DDoS features
- Enable/Disable UTM Security Profiles

Additional features added in v1.3

- IPv6 Policy Configuration
- Firewall Port Forwarding (Destination NAT)
- APIC Dynamic EPG Notification
- Monitor Fortigate Devices (Health) Status
- Fortigate Device Packet Statistics on physical port

Unsupported Features

The following features normally found on FortiGates are not supported through the FortiGate Connector for Cisco ACI.

- Proxy Policy
- SSL/SSH Inspection
- FortiGate WAN load balance link.
- Administrator profile for limited access of different administrator accounts.
- Firewall port forwarding (destination NAT).
- Firewall logging: allowed traffic, security events, all sessions, etc.
- Firewall packet capture.
- Firewall with FortiGuard DDNS.
- Other Firewall features not specifically listed as supported.

The unsupported features on APIC may still be used on FortiGate outside of the APIC control; the user must login to FortiGate to configure, monitor, and debug. However, any conflict with the operations from APIC may cause malfunction.

Supported Fortinet Products

The supported Fortinet products refers to those that are compatible with the FortiGate Connector for Cisco ACI software, and will properly integrate into the Cisco ACI. The products are separated into models and firmware but it is an “and” set of parameters. In order to be supported the Fortinet product has to be one of the listed models running supported firmware.

Models

FortiGate Connector for Cisco ACI v1.3 supports the following predefined models:

- FG-300D
- FG-600D
- FG-900D
- FG-1000C
- FG-1000D
- FG-1200D
- FG-1500D
- FG-3000D
- FG-3100D
- FG-3200D
- FG-3700D
- FG-VM

Unknown models

The use of FortiGate Connector can be attempted with any FortiGate model, but do so with caution. Only those listed above have been confirmed. If an unknown model of FortiGate is used, the user needs to verify port names match the real FortiGate model.

Firmware Versions

FortiGate Connector v1.3 for Cisco ACI is compatible with the following FortiOS firmware:

- FortiOS 5.4 and above

Prerequisites

Cisco Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied within the Cisco environment.

One of the following Cisco ACI environments needs to be in place:

- Cisco ACI v1.2(2h) or later

Within the Cisco ACI, the following configurations need to be completed before Layer 4 -7 Services (in this case, the FortiGate Connector) can be deployed:

- Creation of Access Policies configuration under Fabric menu
- Creation of any need Tenant(s)
- Creation of Network(s) (including Bridge Domain)
- Creation of Application Profile(s)
- Creation of End Point Group(s)
- Creation of Contract(s)
- Create OSPF L3Out (Only if OSPF is required)

For detail, please consult Cisco APIC deployment Guide.

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy.html

FortiGate Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied on the FortiGate side of the equation.

Physical Firewall

1. Configure administrator user name and password.
2. Enable http/https on mgmt. port.
3. Configure IP address in mgmt. port.
4. Enable VDOM-Admin globally.
5. Configure Port-Group if needed.

VM Firewall

1. Assign network ports before start VM
2. Configure administrator user name and password.
3. Enable http/https on mgmt. port.

4. Configure IP address in mgmt. Ports
5. Enable VDOM-Admin globally

Components of the Device Package

To add a network service to ACI fabric, the service's device package needs to be uploaded to APIC. The device package is a zip file containing these components:

Device model or specification

The Device Specification is an XML file called `DeviceModel.xml` that covers descriptions of FortiGate devices, interfaces, connectivity and services. The file contains a hierarchical description of FortiGate devices, including:

- Device functions
- Parameters of each function
- Interfaces/network connectivity information of each function.

Device script

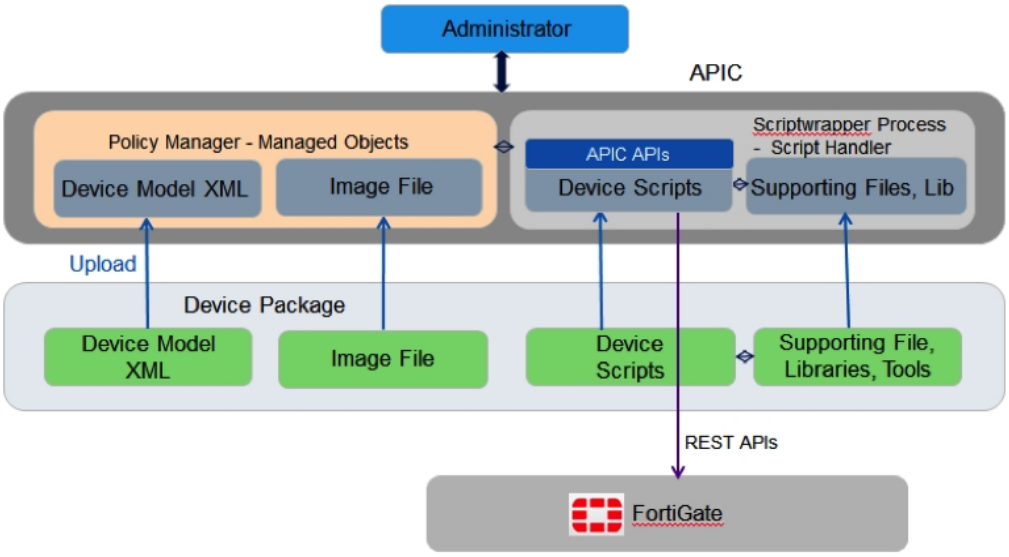
This is a Python file, `DeviceScript.py` with API functions to interface between the Cisco APIC and the FortiGate REST APIs. This Python file is associated by the DeviceModel.xml device specification to device script for APIC.

Directory of supporting files

This component contains supporting Python files, text files and libraries of scripts and tools.

Image file or directory

The directory contains file(s) such as a Fortinet icon (`Fortinet_name.gif`) to be displayed on the APIC management page. There are two types of network service devices which Cisco APIC integrates with. These types of devices are defined by their operation mode. They are either Go Through or Go To. Normally a device as to be preconfigured as one of these types before its imported package is managed by the APIC.


Administrator
APIC
Policy Manager - Managed Objects
Device Model XML
Image File
APIC APIs
Device Scripts
Scriptwrapper Process
- Script Handler
Supporting Files, Lib
Upload
Device Package
Device Model XML
Image File
Device Scripts
Supporting File, Libraries, Tools
REST APIs
FortiGate

Operational modes

There are two types of network service devices which Cisco APIC integrates with. These types of devices are defined by their operation mode. They are either Go Through or Go To. Normally a device has to be preconfigured as one of these types before its imported package is managed by the APIC.

Go Through Mode (Layer 2)

Devices in Go Through mode are considered layer 2 devices (from the OSI model) and are sometimes known as transparent. They are referred to as transparent because while the traffic goes through them and can be affected by them, they are not seen by the network and are not a destination in their own right for the traffic. They do not route traffic. These devices are not referred to by the packet's destination MAC or IP address. In most cases, these devices will only have an address for the purposes of management.

Go To Mode (Layer 3)

Devices in Go To mode are considered Layer 3 (from the OSI model) devices. They can route traffic and they are referenced as the destination in a packet's destination MAC address or destination IP address.

Multi-tenant multi-device support

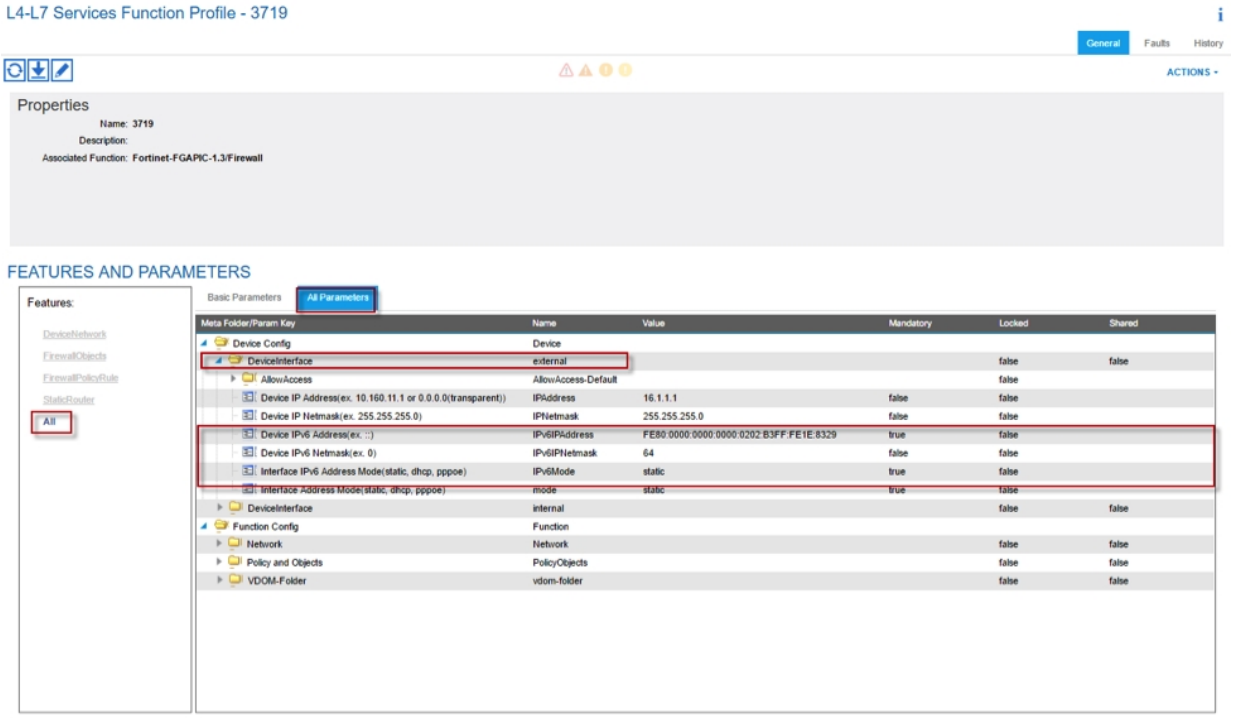
- Multi-tenant Multi-device is typical in the use cases of this project. The support is worth more detailed description. When FortiGate device is added a tenant's L4-L7 services, multi-context aware can be enabled. This indicates to the device package that the L4-L7 device is going to be a virtual device that shares resources with other tenants on the FortiGate. In FortiGate implementation, this virtual device is represented by a VDOM. Under each tenant, multiple such virtual devices can be configured. VDOM name is the virtual device ID generated by APIC when a virtual device is added.
- Each tenant sees all available interfaces and can share interfaces (ports) with other tenants, if it is multi-context aware. For Physical Device under L3 Routed (GoTo) Mode, Tenant can share physical interface as VLAN is used to isolate the physical interface. In VM Device, this is not true. You can only use dedicated VNIC.

New Feature Deployment Guide

IPv6

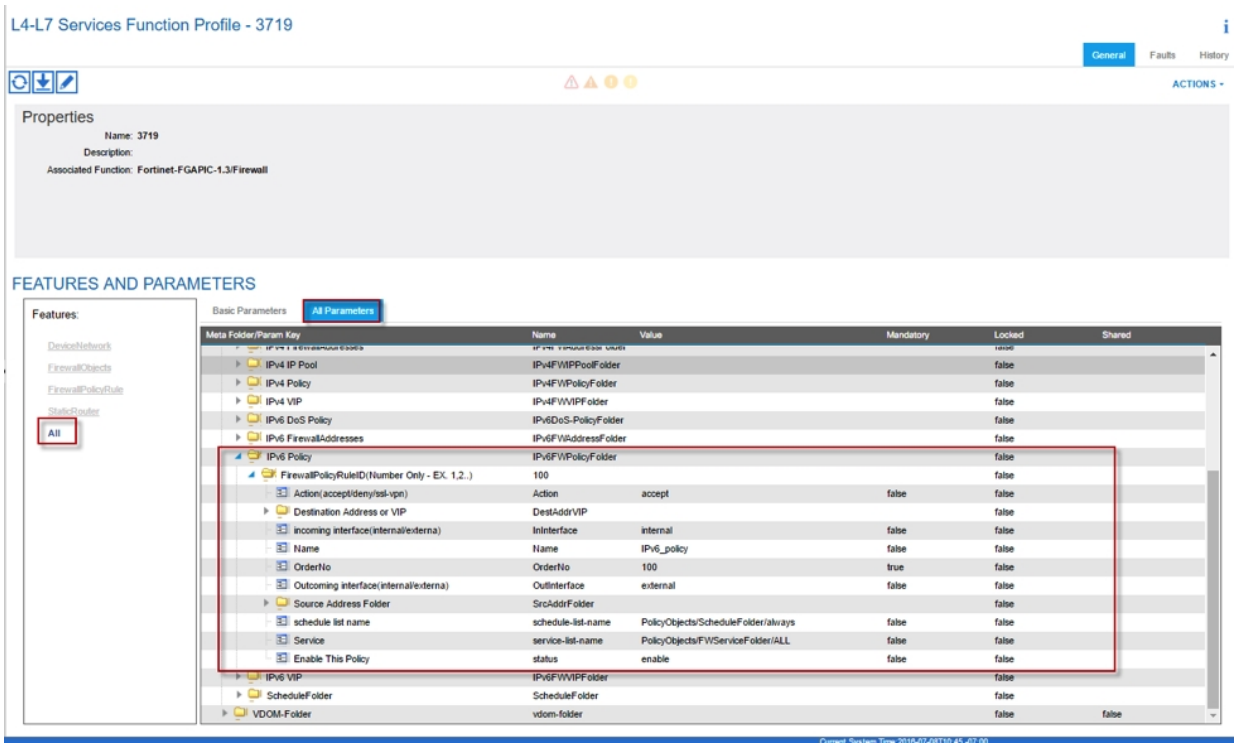
IPv6 Interface Configuration

We now support IPv6 configuration on interface level. Please consult below screen shot.



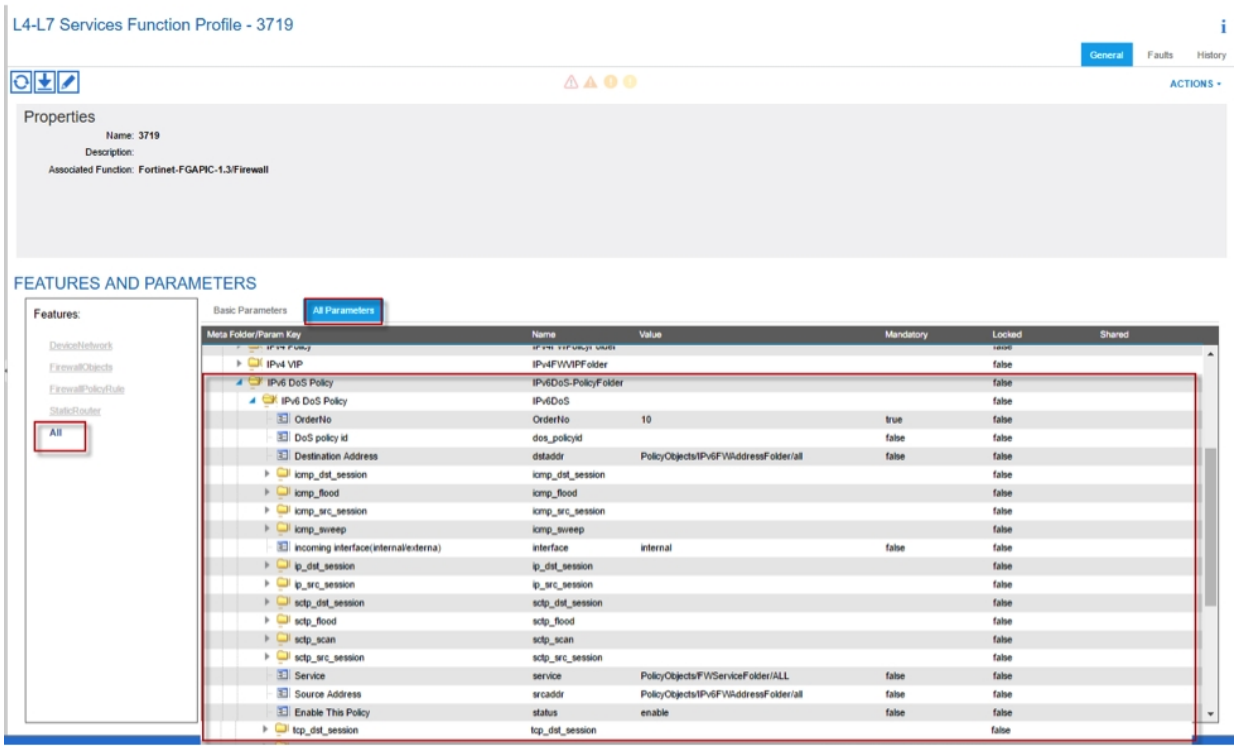
IPv6 Policy

Once we configured IPv6 addresses onto interfaces, we can configure IPv6 policy to enforce the traffic. Please consult below screenshot.



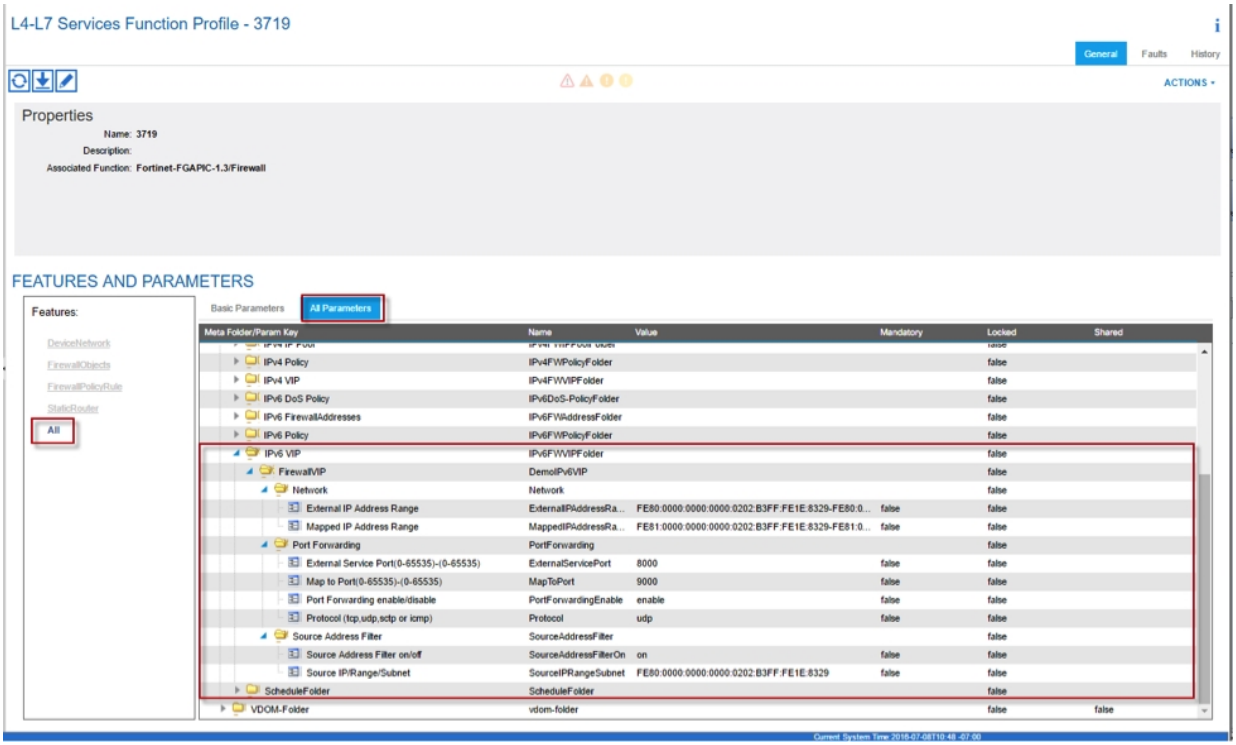
IPv6 Dos

Optionally, we can configure IPv6 Dos feature. Please consult below screenshot.



IPv6 Virtual IPs

In addition, we can configure IPv6 Virtual IP feature which you can apply to IPv6 Policy. Please consult below screenshot.



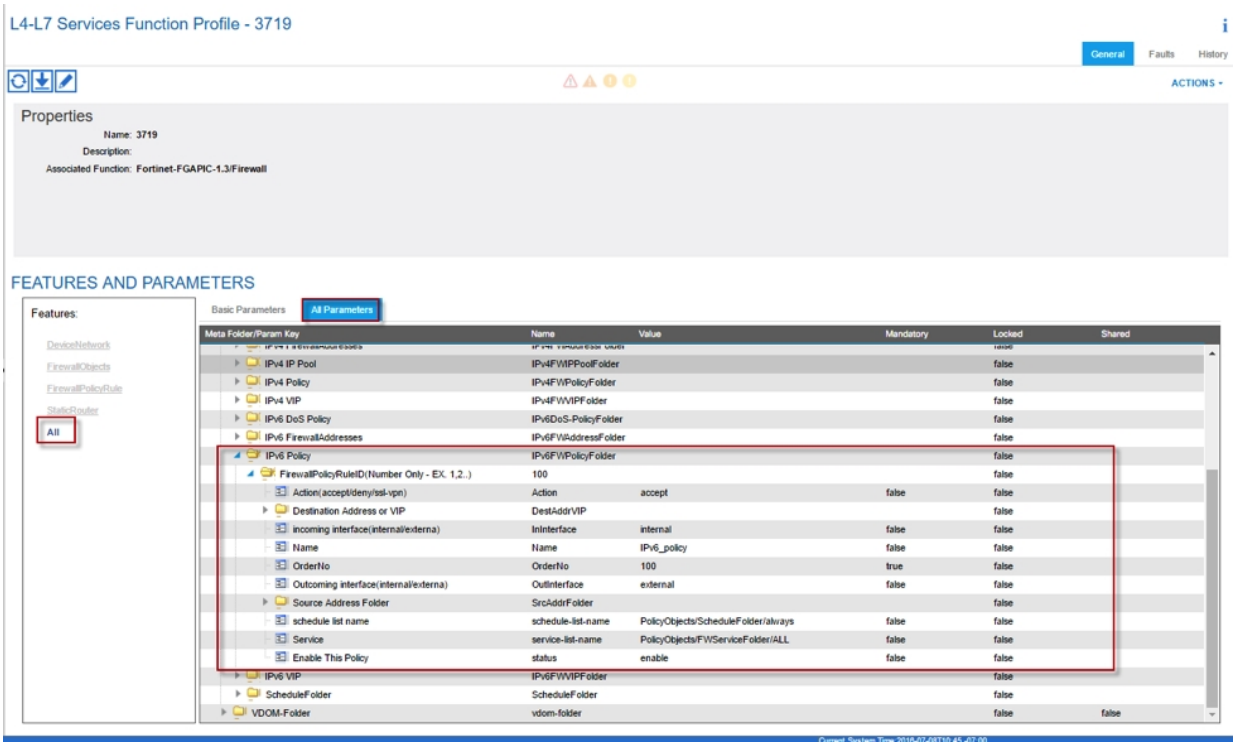
Firewall Port Forwarding (Destination NAT)

IP Pool Configuration

Below screenshot illustrated how to define IPv4 IP Pool. Due to the layout format ACI is providing, we have to list all the sub-features within the IP Pool. Please consult Fortigate Configuration Guide for option(s) that goes with appropriate Sub-feature. Otherwise, we will see error when push configuration from APIC down to Fortigate. From a very high level, here is the break down lay out of the Sub-feature and the accommodated options.

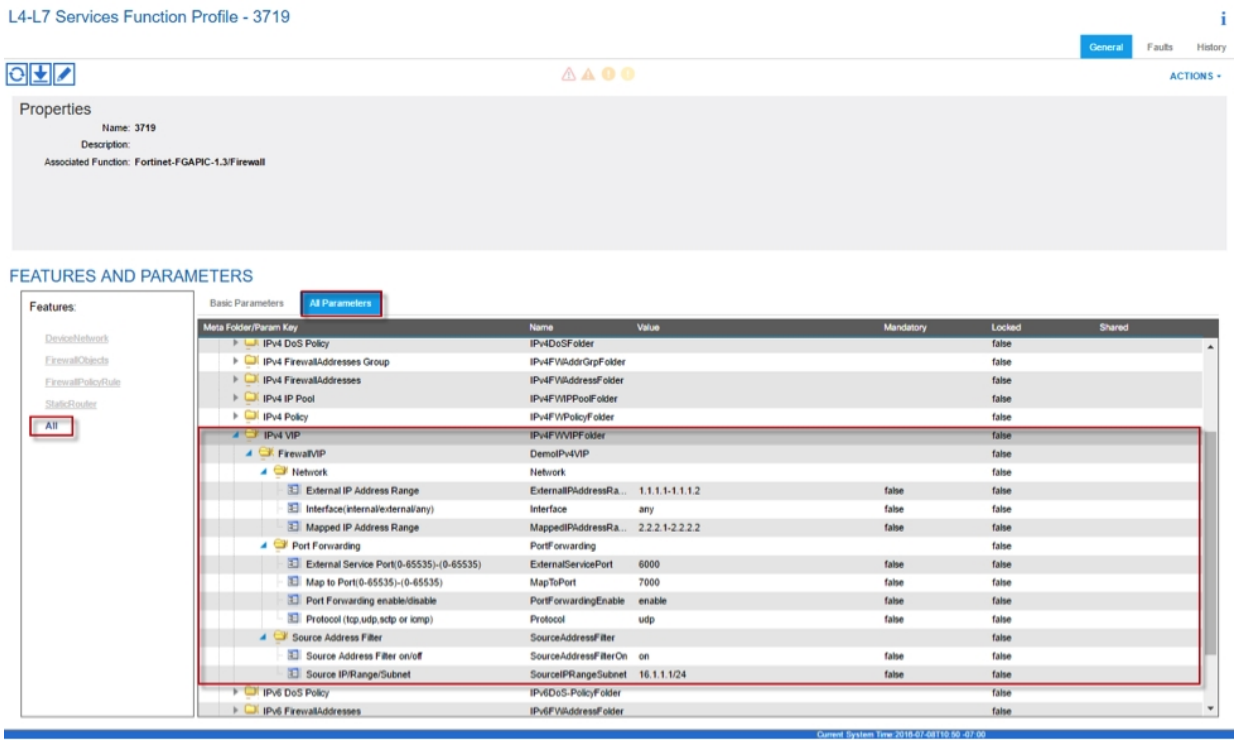
Dynamic IP Pool				
IP Pool type	IPv4 Pool			
Name				
Comments				
Type	Overload	One-to-One	Fixed Port Range	Port Block Allocation
External IP Range	x	x	x	x

Dynamic IP Pool				
Internal IP Range	N/A	N/A		N/A
Block Size	N/A	N/A	N/A	x
Blocks per User	N/A	N/A	N/A	x
ARP Reply	x	x	x	x



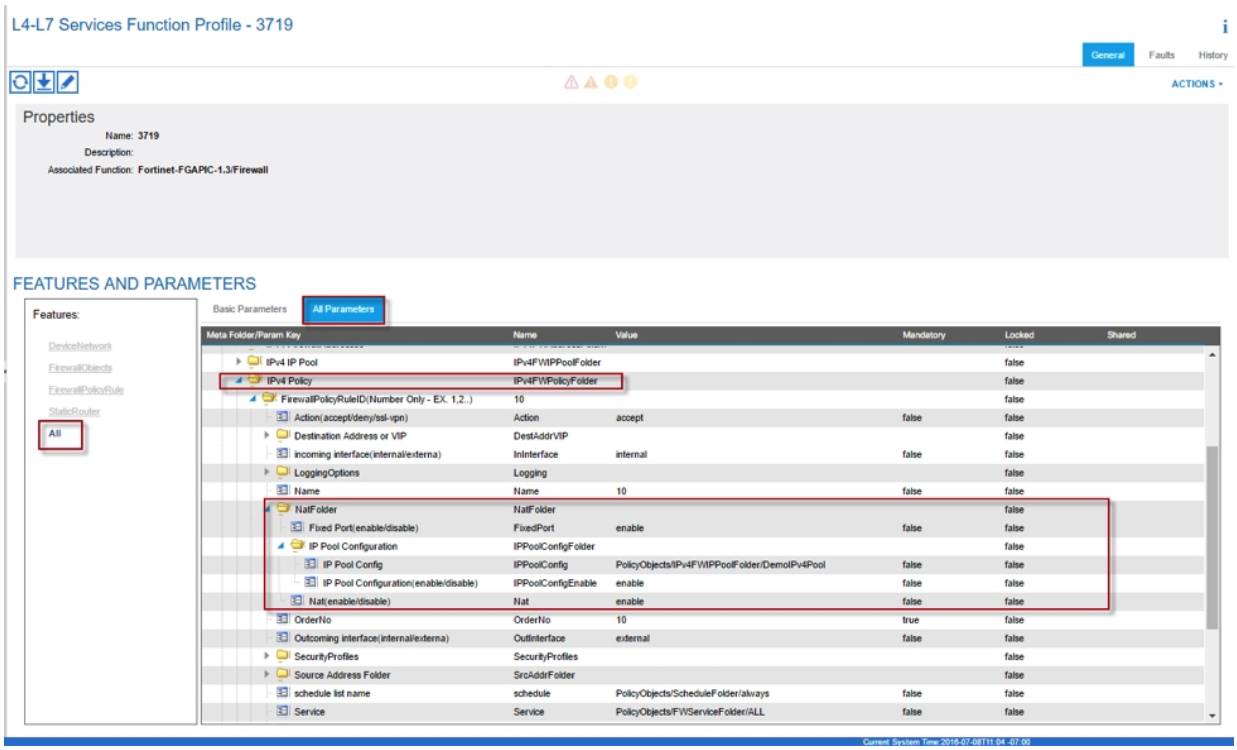
IPv4 Virtual IPs

IPv4 Virtual IP Pool can also configure for DNAT feature. Please consult below screenshot.



DNAT Enable on Policy

Once above DNAT sub-components are configured, we can apply them to the Policy level. Please consult below screenshot for reference.



Device Health

From L4-L7 Device level, we can obtain the Fortigate Device Health. Navigate to ***L4-L7 Services> L4-L7 Devices>Device Name> Concrete Device> Health Tab***, you can obtain the device health. Please consult below screenshot for reference.

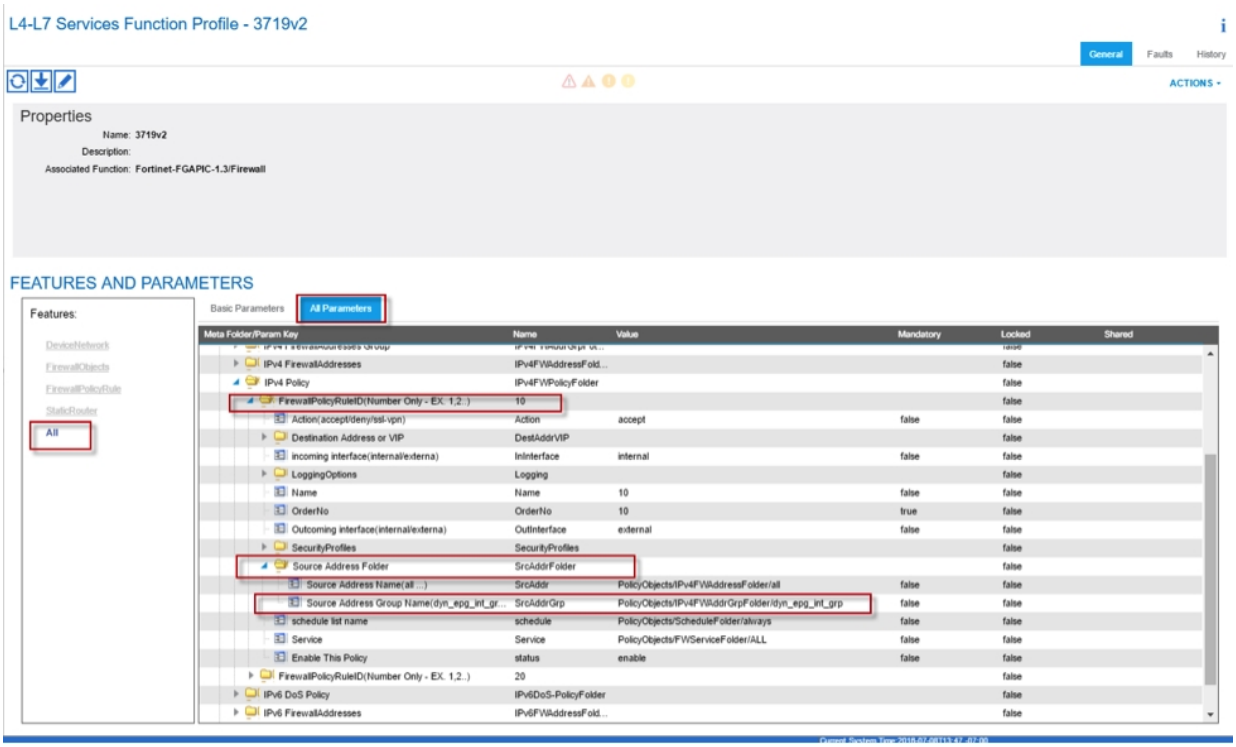
Interface Statistic

From L4-L7 Device level, we can also obtain the Fortigate Interface Statistic. Navigate to ***L4-L7 Services> L4-L7 Devices>Device Name> Concrete Device> Interface>Stats Tab***, you can observe interface statistic by enabling various statistic indicator such as RX/TX…etc. Please consult below screenshot for reference.

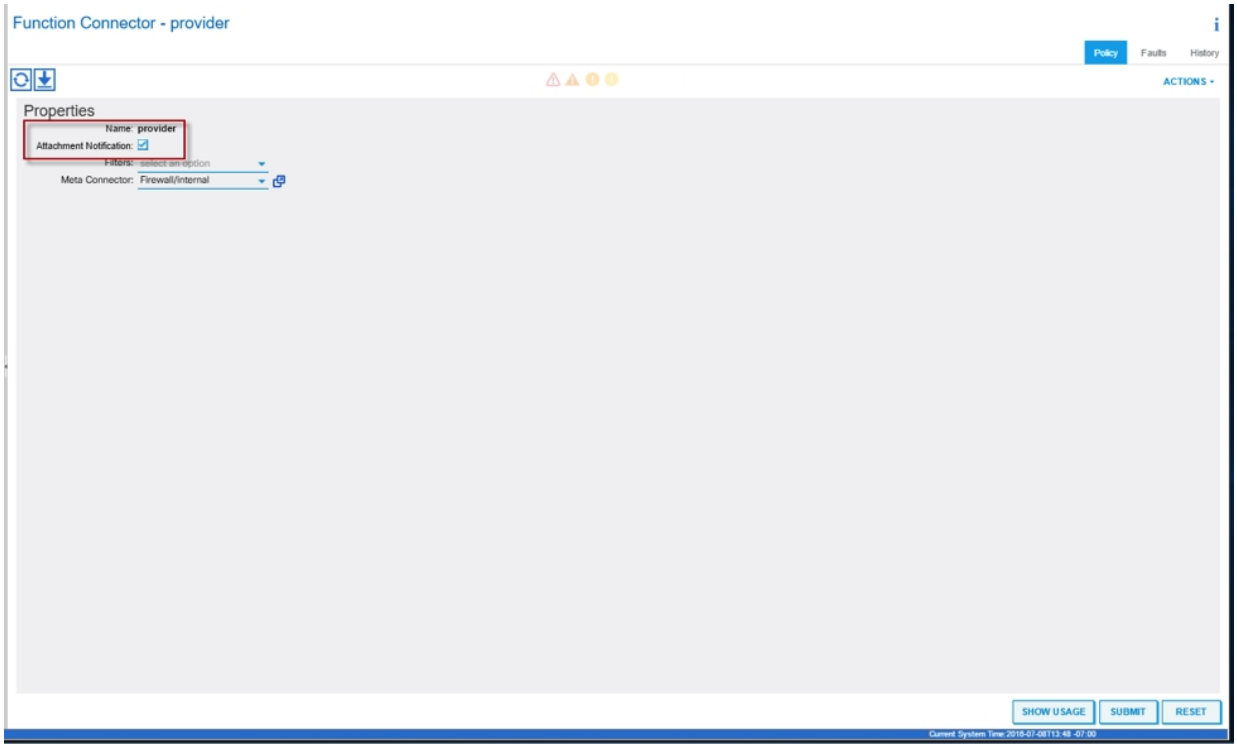
Dynamic EPG Notification

This feature allowing us to dynamically update of object group membership, where it corresponds to an End Point Group (EPG). You can dynamically add IP addresses/subnets based on endpoint/network attachment notification by ACI.

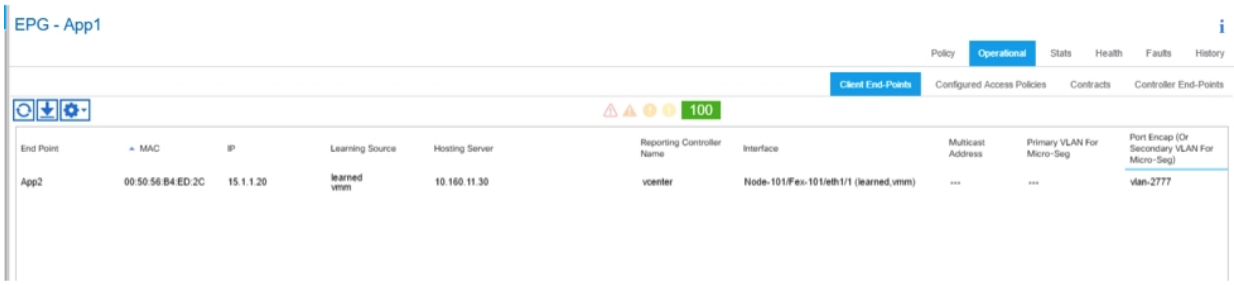
For this feature, we have created two groups "`dyn_epg_ext_grp`" and "`dyn_epg_int_grp`" which you can apply to the policy source field. When an end point is detected, notification will received from ACI and the endpoint IP will added to this membership group where policy will be applied.



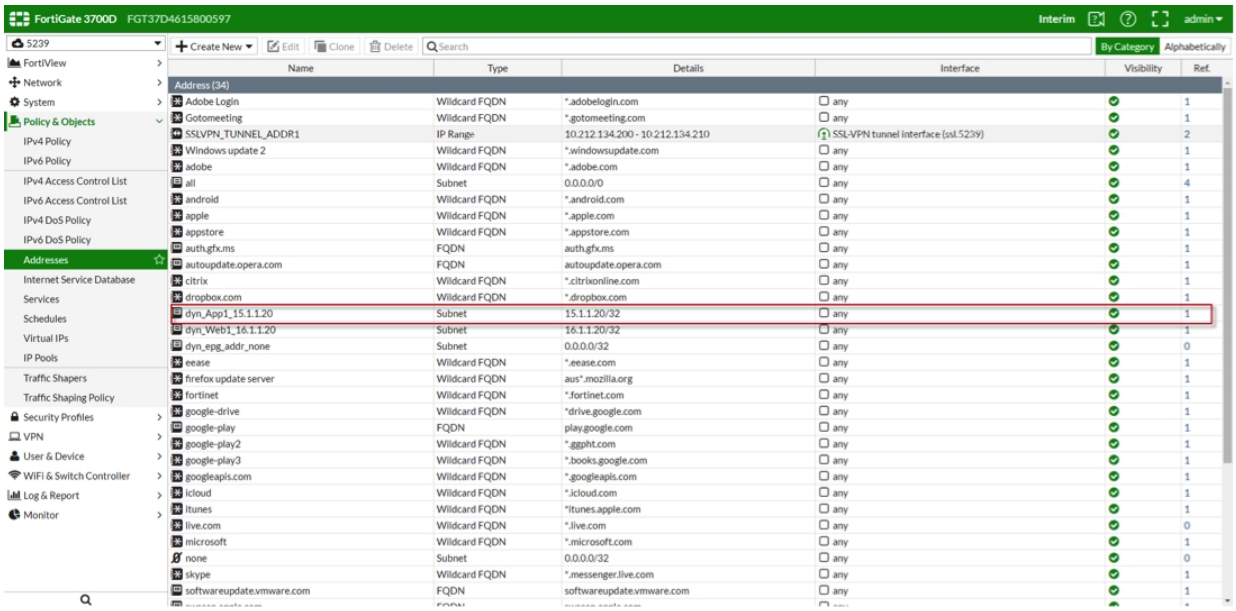
From above example, we added "`dyn_epg_int_grp`" to ***Source Address Group Name*** field under Policy 10



From ***L4-L7 Service Graph Template>Function Node>Consumer/Provider***, we have to check the box ***Attachment Notification*** in order for ACI to notify Fortigate when Endpoint attached to the Group.



EPG Operational level indicated Endpoint attached to the EPG.



Fortigate Appended dynamic added Endpoint to the Group.

Supported use scenarios

Physical Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Virtual Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Deployment Procedures

Below sections, we will walk through the high level of how to deploy a service insertion as well as detail procedures of how to perform each steps.

Device package installation

To successfully deploy Fortigate Connector into Cisco APIC, customers need to perform the following steps:

1. Import Device Package
2. Add L4-L7 Device
3. Create Functional Profile
4. Create Service Graph Template
5. Deploy Service Graph Template.

Service Deployment

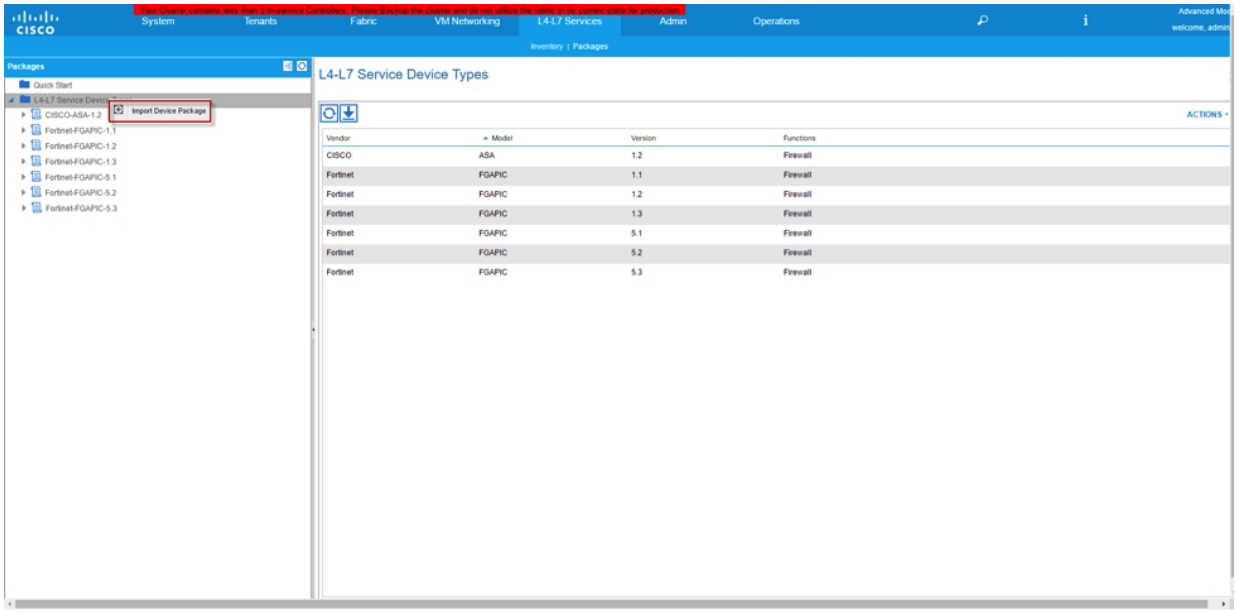
According to the APIC deployment guide, a service device introduces a Layer 4 to Layer 7 service by this typical procedure:

1. Import the device package of the service device,
2. Configure a tenant who asks for network services,
3. Register the device and its logical interfaces,
4. Configure logical device parameters,
5. Configure a layer 3 network,
6. Configure a bridge domain,
7. Configure an application profile,
8. Configure a physical domain (or VMM domain),
9. Configure a VLAN pool,
10. Configure a contract
11. Configure a management endpoint group (EPG),
12. Configure a service graph template,
13. Select default service graph template parameters,
14. Attach the service graph template to a contract
15. Configure additional configuration parameters.

To add a support of a non-Cisco firewall device in the Cisco ACI fabric based data center, a device package should be developed for the APIC. Then the remaining task is standard APIC deployment of a network service device.

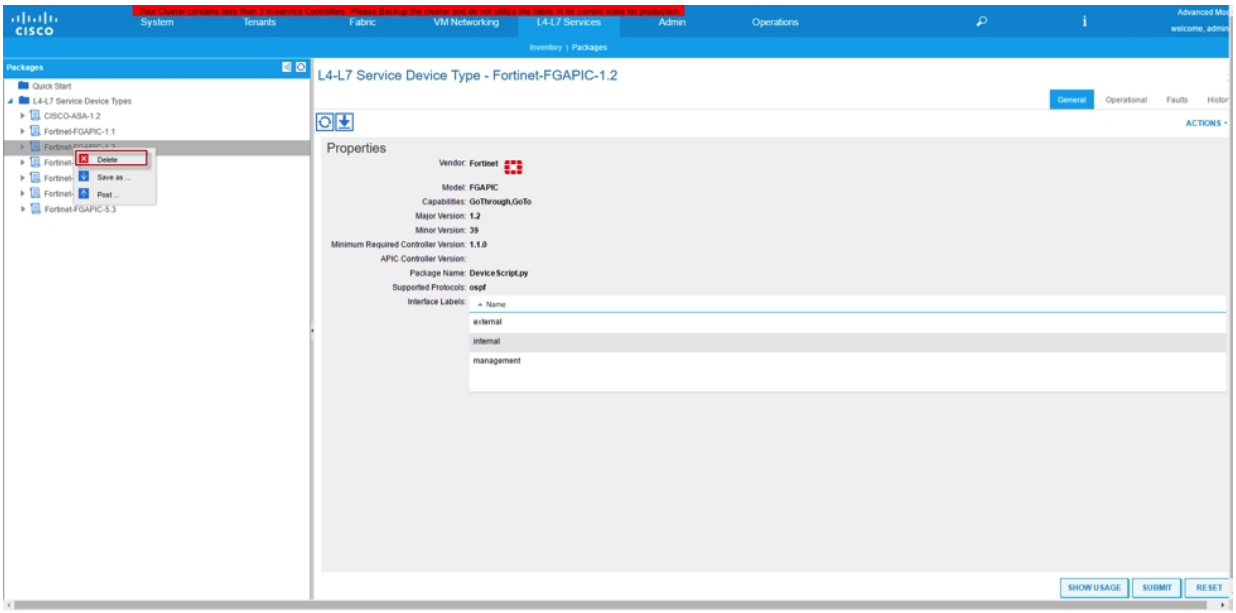
Importing the Device Package

1. Download Device Connector Package from Fortinet Support Web (URL) site to local storage.
2. From APIC menu, Navigate to ***L4-L7 Services > Packages*** and right click on ***L4-L7 Device Type*** on the left hand panel. Select ***Import Device Package***



Remove Device Package

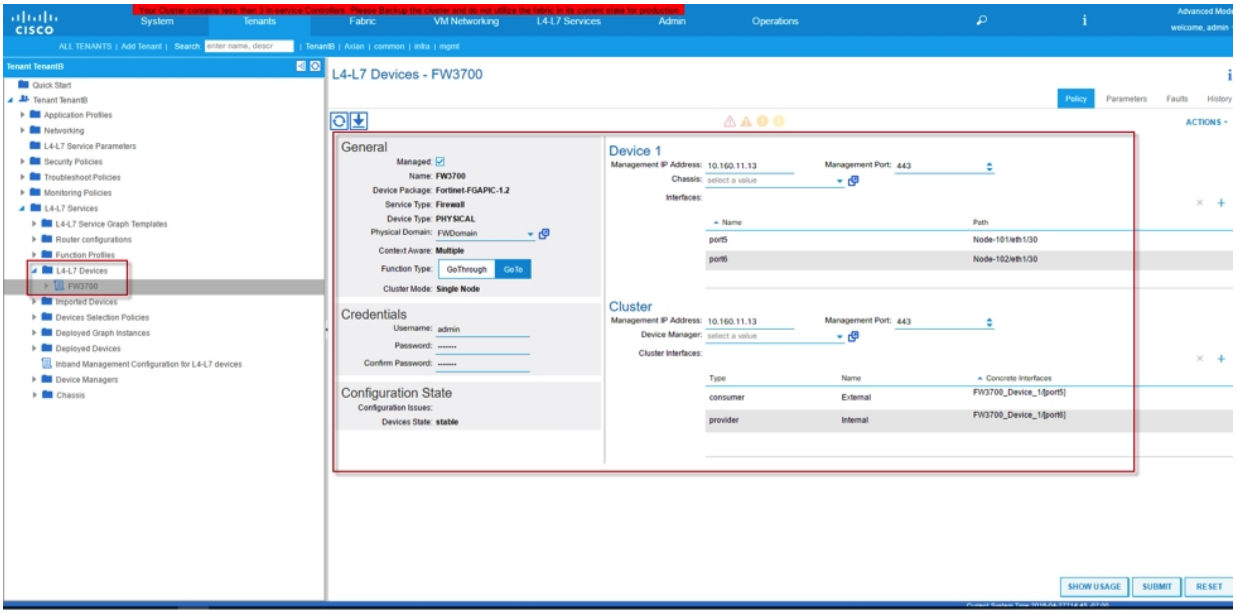
To remove Device Package, navigate to ***L4-L7 Services > Packages*** and right click on the Device package on the left panel and select ***Delete*** option.



Basic Steps to add Fortinet Firewall L4-L7 Virtual Device

Add L4-L7 Device

Within Tenant, Expand ***L4-L7 Services > L4-L7 Devices***, right click on mouse and select "***Create L4-L7 devices***"



GENERAL

Field	Description / Options
Name	Name of the Device
Device Package	Select Device Package from drop down list
Model	<List of the supported models>
Mode	• Single Node / HA Cluster
Function Type	• GoThrough (L2) • Goto (L3)

CONNECTIVITY

Field	Description / Options
Physical Domain or VMM Domain	Select from drop down list Domain which you should have configured during APIC Access Policies setup
APIC to Device	• Out-of-Band • In-Band

CREDENTIALS

Field	Description
Username	<login name to the Fortigate>
Password	<Password to login to Fortigate>
Confirm Password	<Password to login to Fortigate>

Device 1

Field	Description / Options
Management IP Address	<IP address to connect to Fortigate>

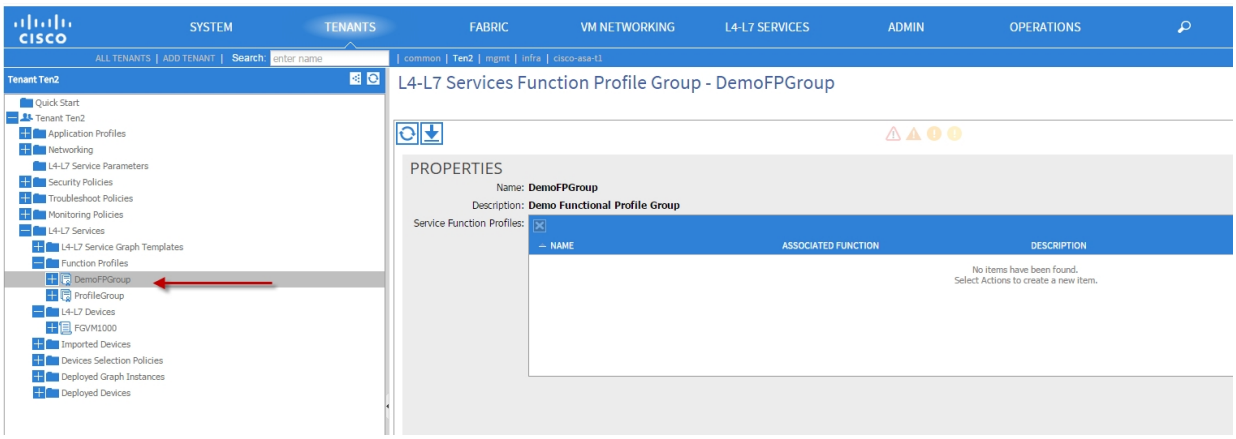
Field	Description / Options
Management Port	• http • https https is the prefer method
Connects To	• Port (Default), PC, VPC
Physical Interfaces	Click on “+” sign to add interfaces connecting from APIC to FortiGate
Name	Select from Drop down list to select port. (If using Port Channel, please type in the correct Port Channel name ex:PO1, PO2..etc.)

Cluster

Configure all the fields same as Device 1, with exception to Cluster Interface.

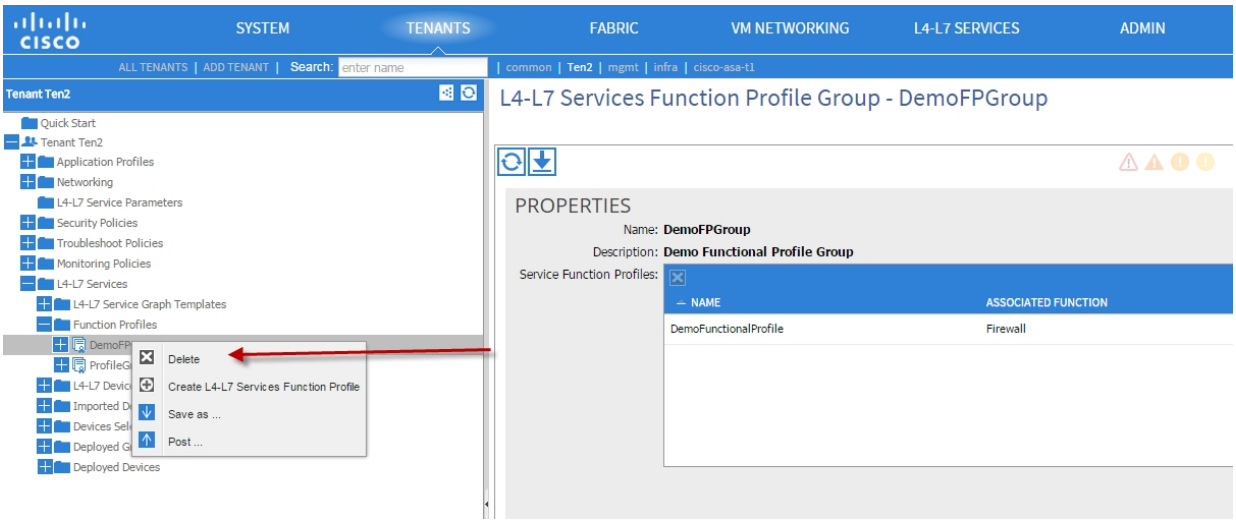
For Cluster Interface, click the “+” icon to add logical device interfaces.

Create Functional Profile Group



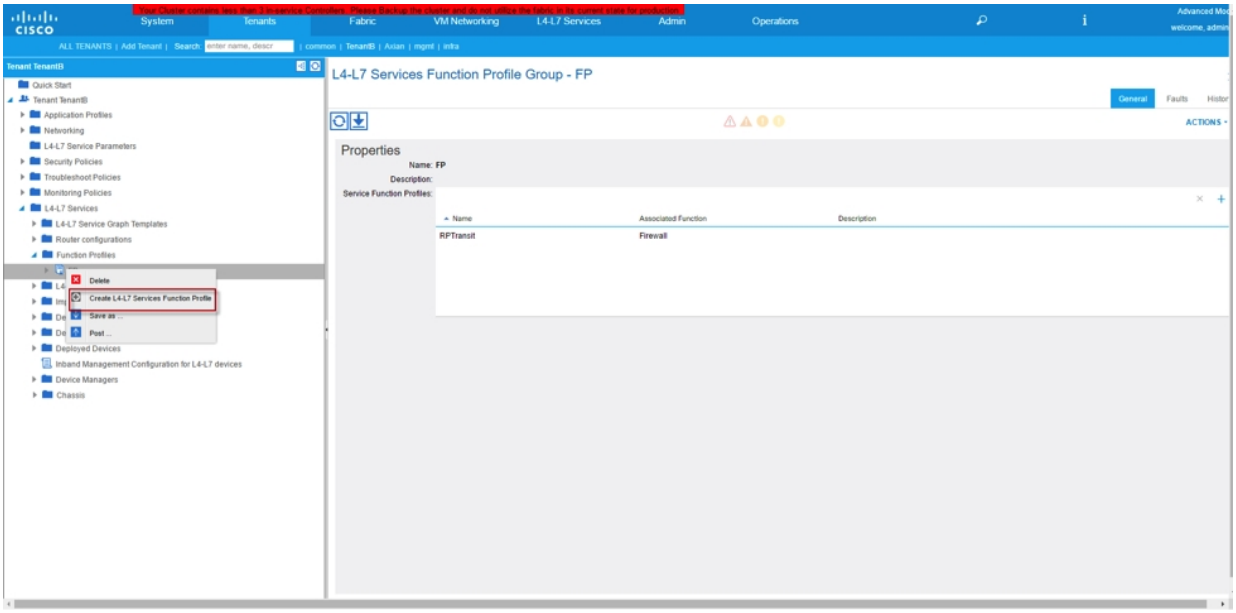
Remove Functional Profile Group

To remove Functional Profile Group, navigate to ***Tenant > L4-L7 Services > Functional Profiles*** and right click on the Functional Profile group name listed on the left hand panel and select ***Delete*** option.



Create a Function Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation under “Features”:

Device Network:

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. If user intends to have multiple legs deployment scenario, this is where he/she can add additional interfaces with unique name.

Beginning with FortiGate Connector v1.2, the device package no longer has the option to select VDOM mode and VDOM name. Instead, the VDOM name is automatically generated based on virtual device ID from APIC; the VDOM mode is based selection of Go-to mode and Go-through mode during the device creation. If Go-to mode is selected, user must input IP addresses and subnet mask for each interface; if Go-through mode is selected, user must leave IP address field untouched.

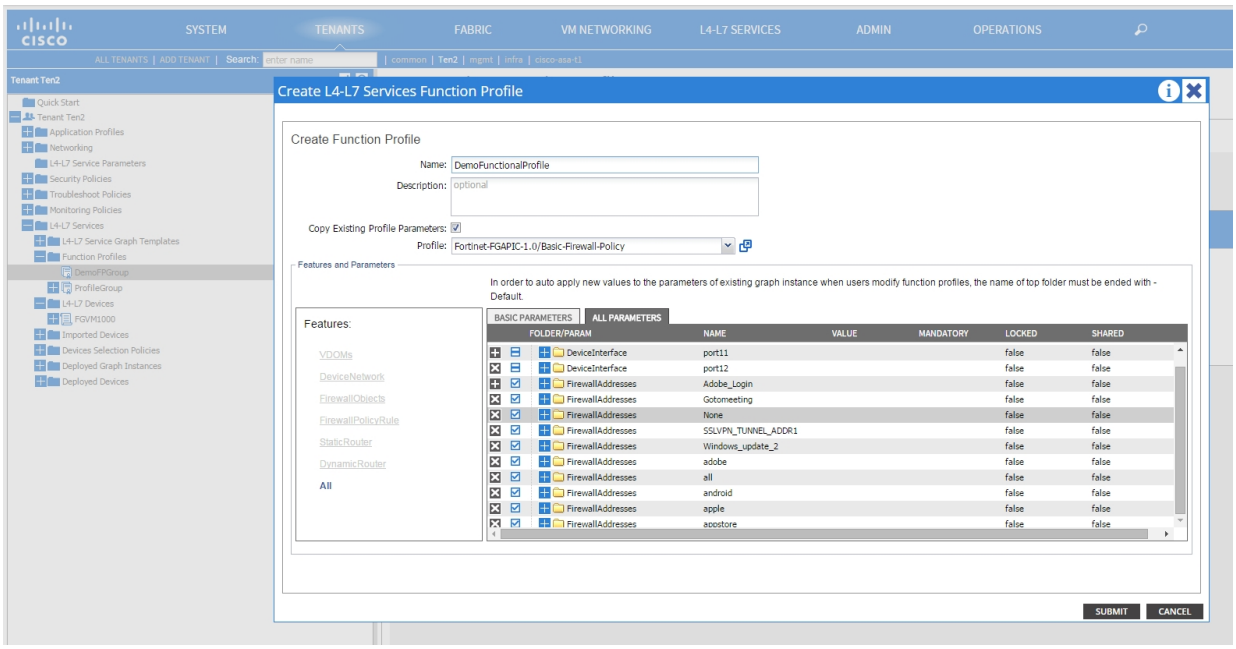
Function Config

Function Config consist of:

- **Network**
  - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
  - This folder is the container for following list of Folders:
    a. FWServiceFolder – Firewall Service Object container
    b. IPv4/IPv6 DoS Policy – Dos Policy configuration
    c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
    d. IPv4 Policy – Firewall Policy Rule container
    e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    f. ScheduleFolder – Schedule container
- **VDOM-Folder**
  - VDOM internal and external interfaces

Review

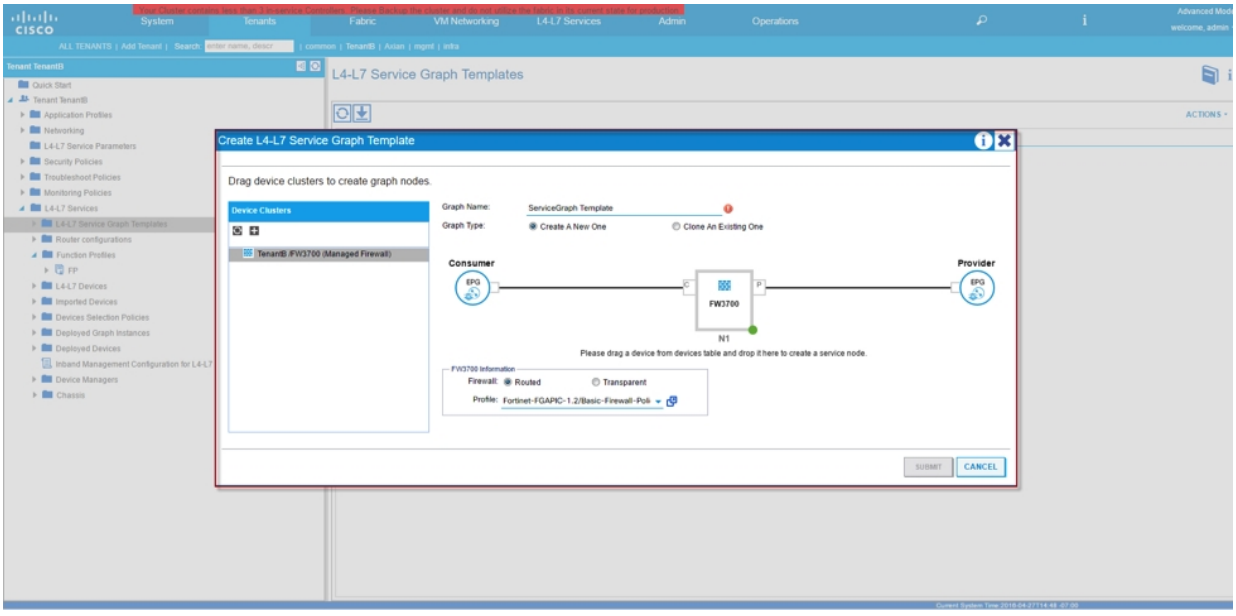
All Field display all the fields in the features listing. If you are satisfy with all your inputs, then hit the submit button to complete your creation of Functional Profile template.



Service Graph

Create Service Graph

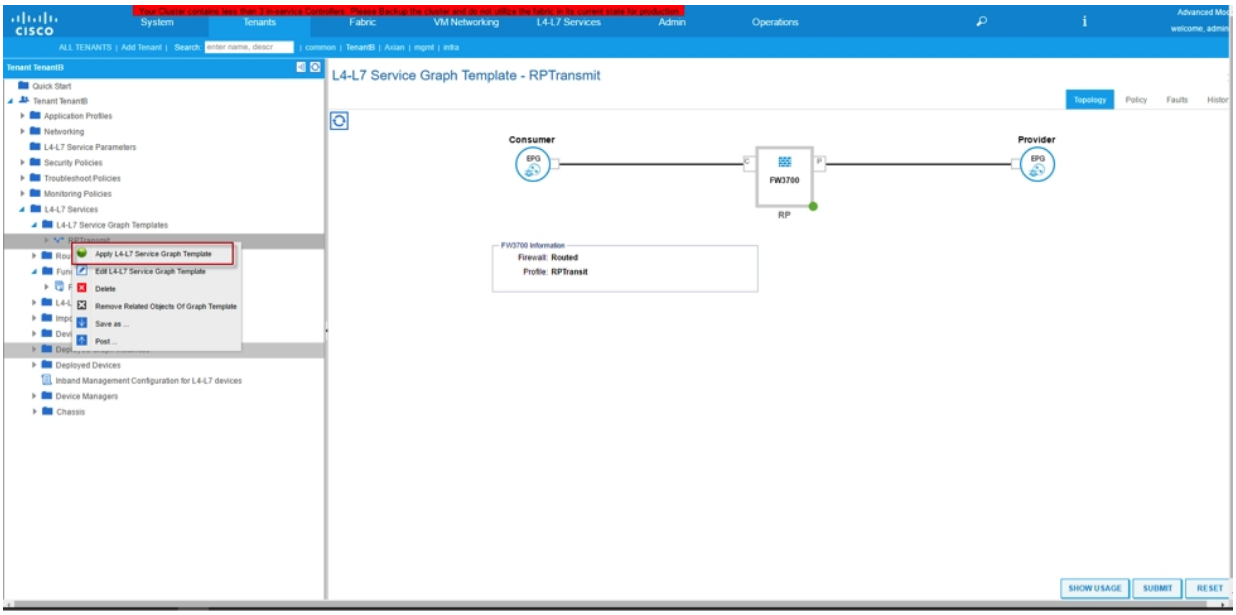
Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.



Right Click on ***L4-L7 Service Graph Template*** to create a Service Graph.

Deploy Service Graph

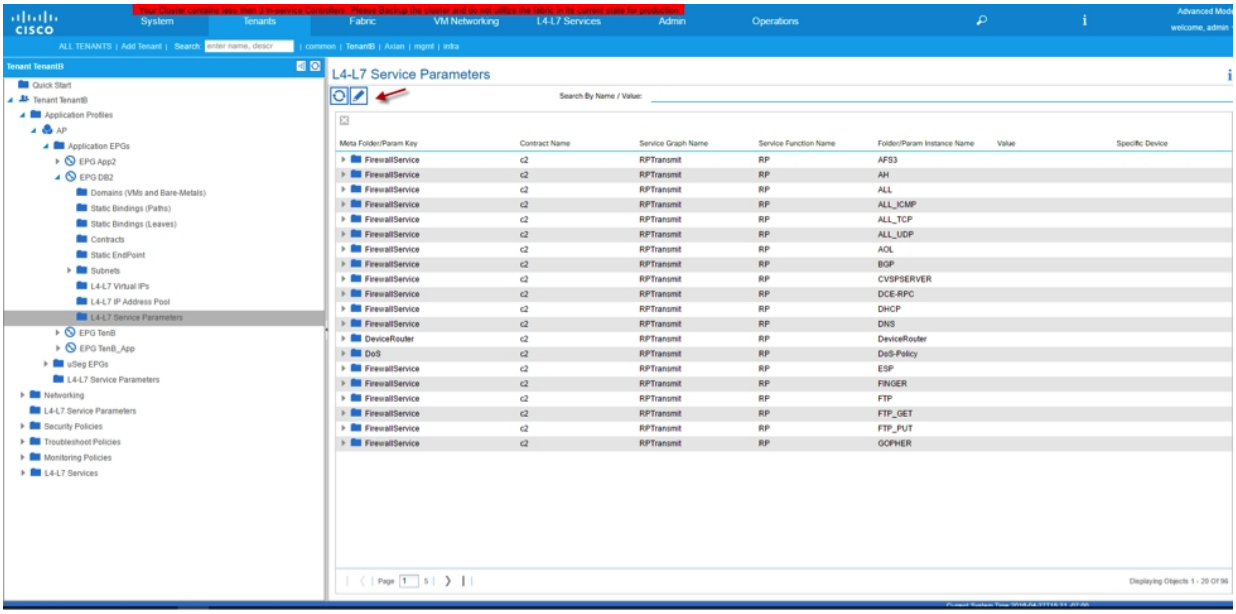
Once we combined the Firewall configuration and associated device together, we are ready to deploy the service Graph to create a VDOM automatically.



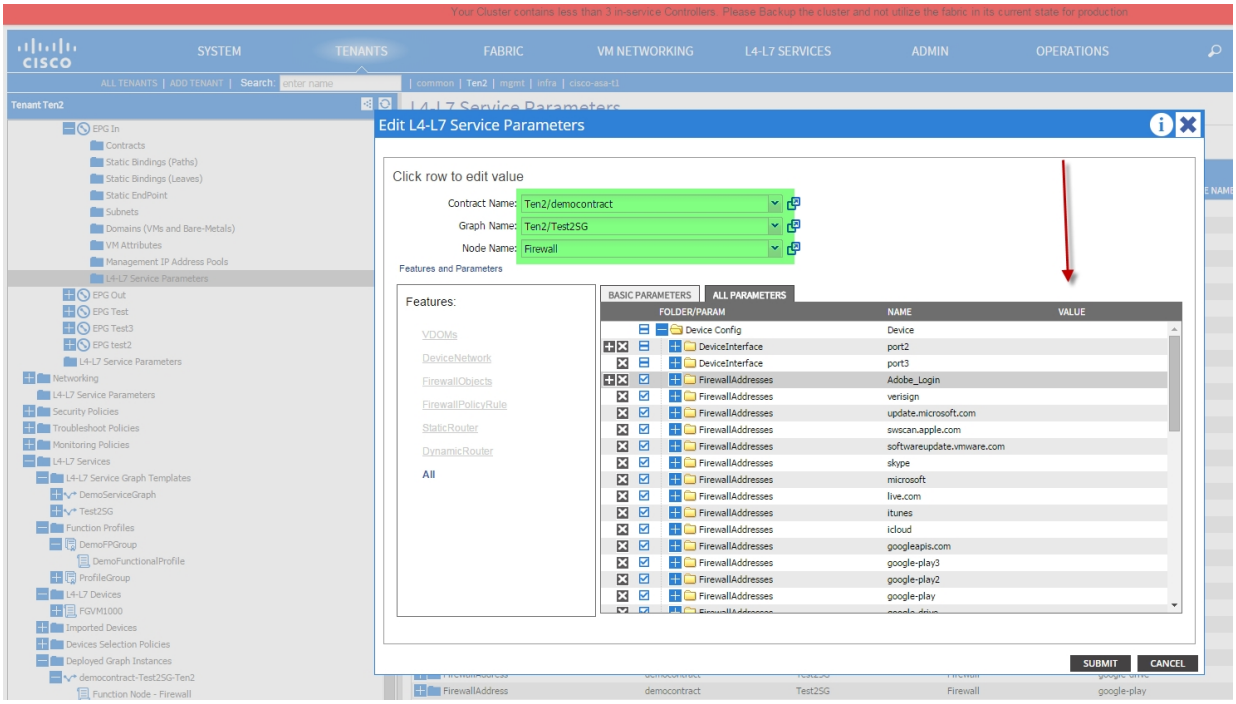
Right Click on Service Graph defined from above and select ***Apply L4-L7 Service Graph Template.***

Modify Service Graph

1. From ***Tenant>Provider EPG>L4-L7 Service Parameters*** and select the pen icon, which will lead you into edit mode to modify parameters on deployed Service Graph.

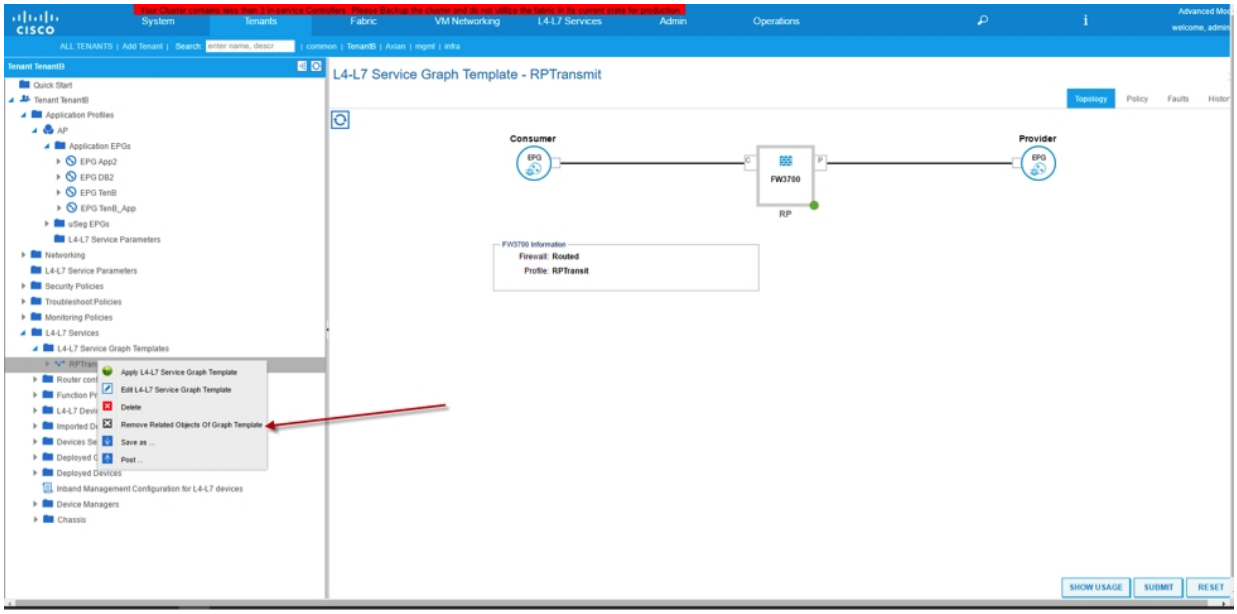


2. On the next screen, select the Contract name, Graph Name and Node name from the drop down list and all the associated Service Graph Parameters will be displayed.
3. Expand the field you want to make modification and change the appropriate value from the drop down list and then hit submit.



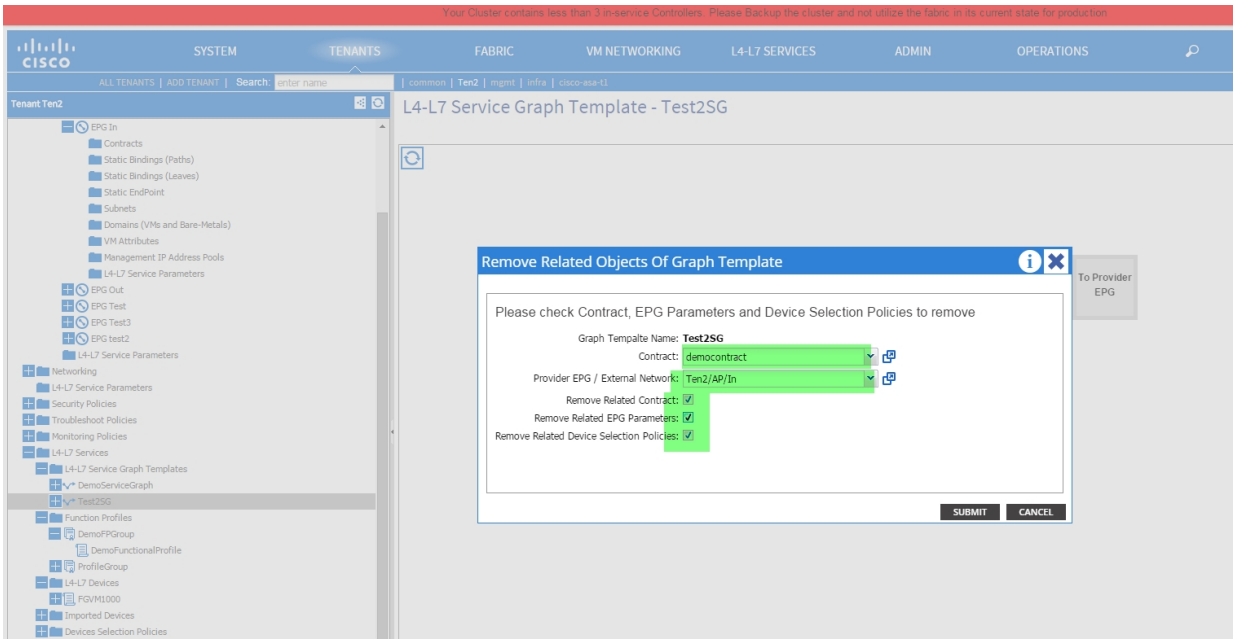
Remove Service Graph

1. Navigate to ***Tenant>L4-L7 Services>L4-L7 Service Graph Templates***. Right click on Service Graph template and select***Remove Related Objects Of Graph Template.***



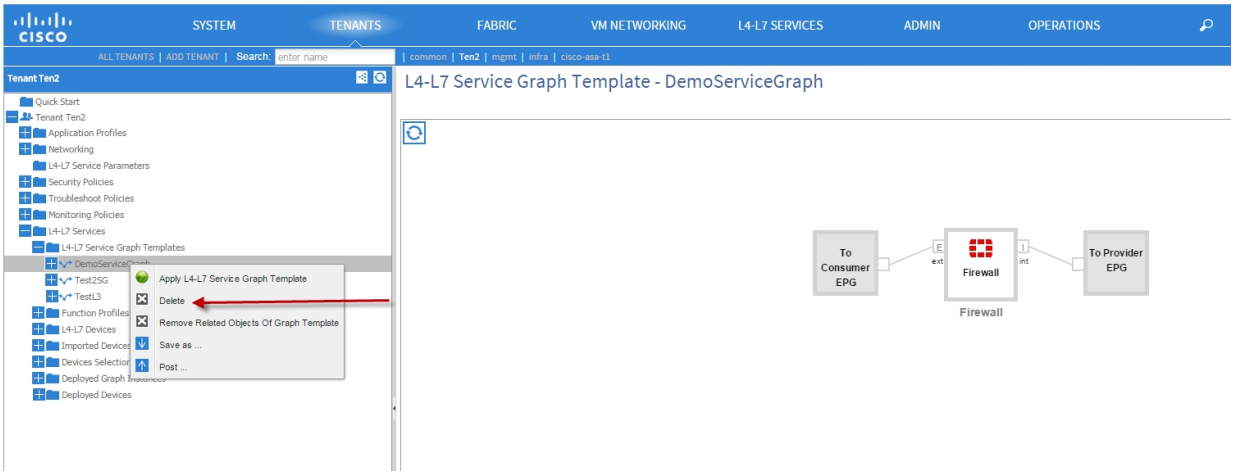
2. Select ***Contract and Provider EPG*** from the drop down list and check all 3 boxes:
   - ***Remove Related Contract***
   - ***Remove Related EPG Parameters***
   - ***Remove Related Device Selection Policies***

   Hit *Submit*. This will remove all the related objects for this Service Graph.



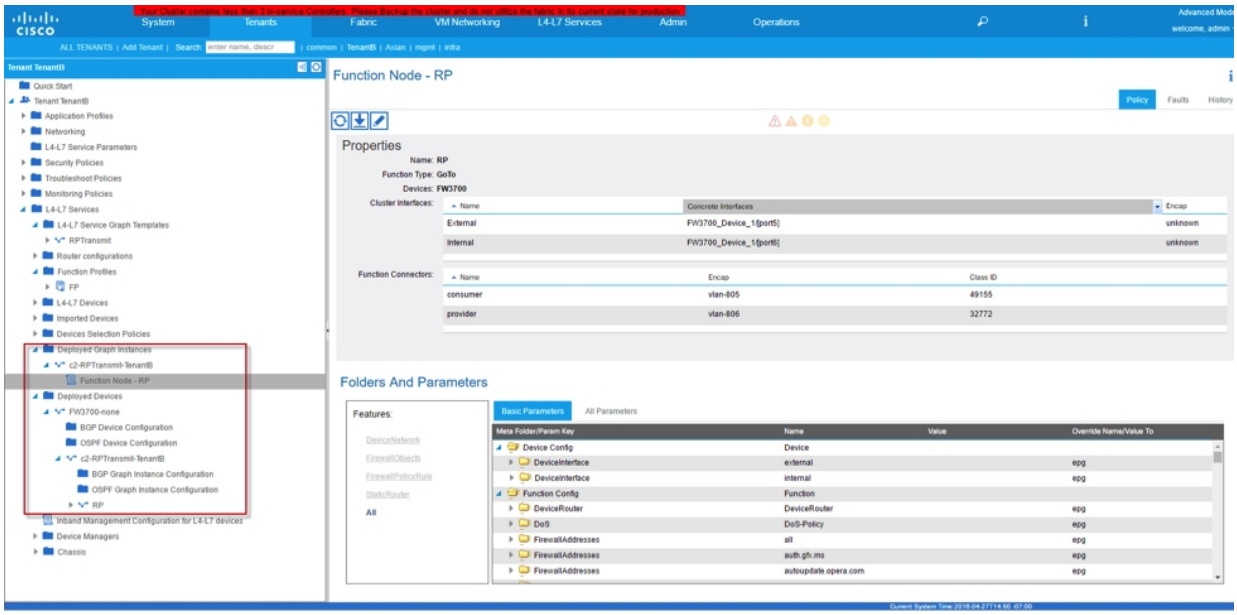
Delete the Service Graph

1. To delete the Service Graph Template, navigate to ***Tenant > L4-L7 Services > L4-L7 Service Graph Templates***.
2. Right click on template name listed on the left hand panel and select ***Delete*** option.



Service Graph deployed

Once the service graph is deployed, the Fortigate device will received configuration through REST API commands from the Cisco APIC. Below figure shows a successful service graph deployment. The Interface configuration such as vlan, IP..etc and firewall policies are all being programmed onto the Fortigate. From this point forward, any update is continue to be manage by Cisco APIC until the service graph is remove.



Installation Variations

Deploying Data Center Layer 2 Segmentation with Cisco ACI and FortiGate

Pre-requisites

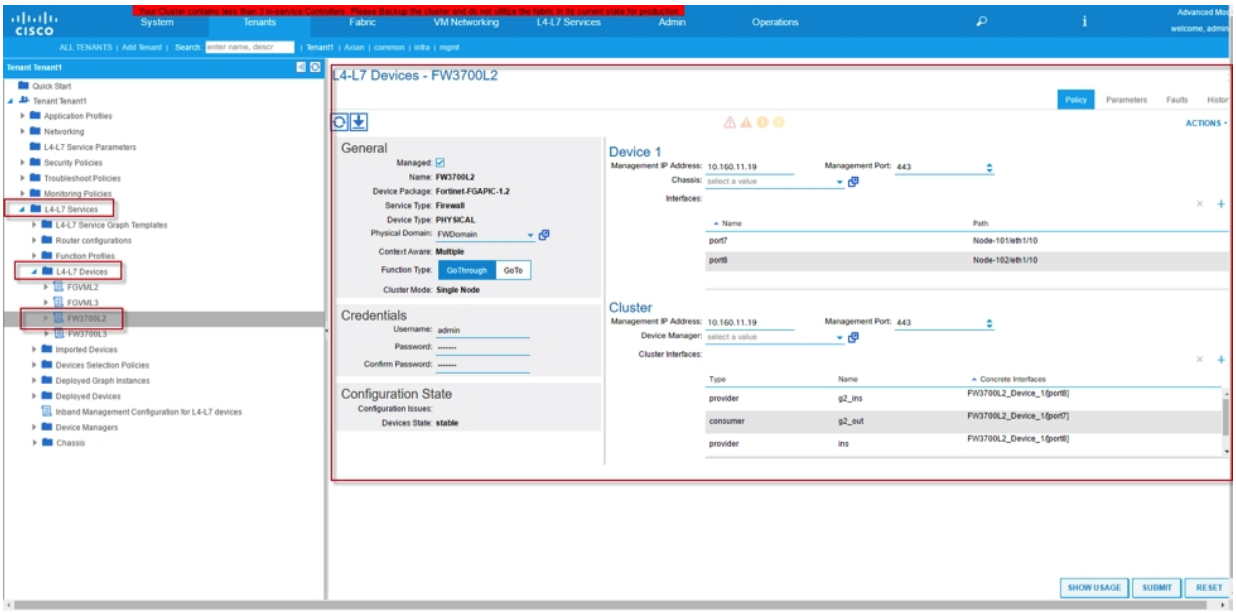
- Fabric Access Policies creation relating to
  - Vlan Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer 4-7 Device Package has imported into Cisco APIC

Work Flow

1. Create L4-L7 Device with Go-through Mode
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

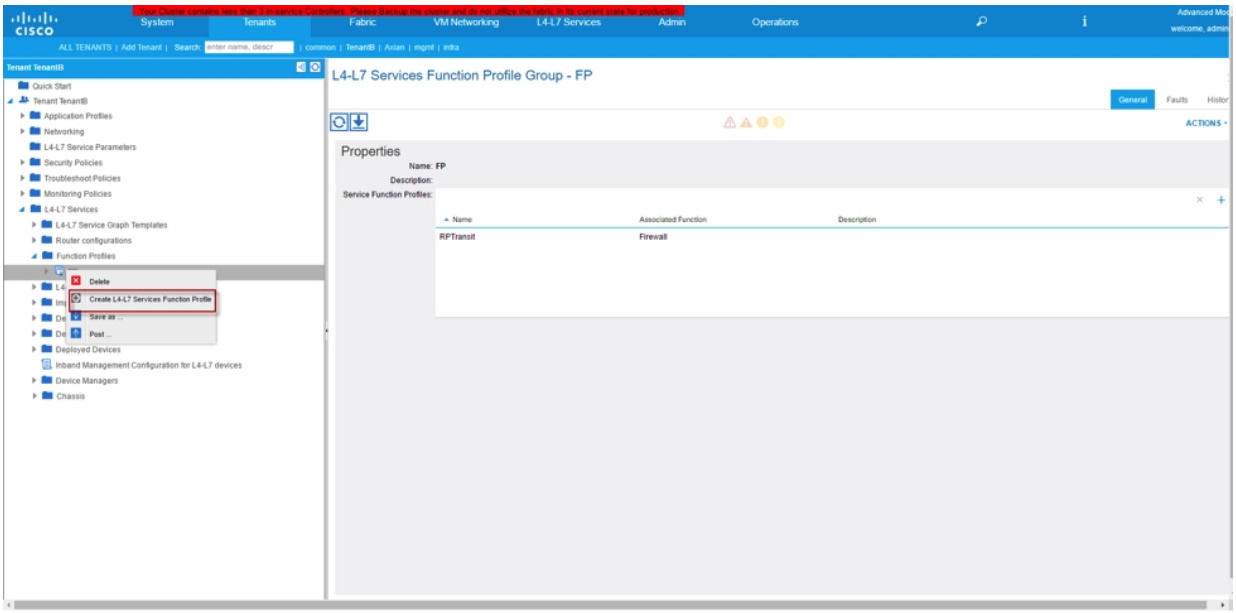
Configuration

Create L4-L7 Device with Go-Through mode on Cisco APIC



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy, such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation:

Device Config

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. These are the interfaces (typically external and internal) that will be associated to the VDOM. If user intends to have multiple legs deployment scenario, this is where additional interfaces with unique names can be added.

User must leave IP address field untouched in Go-through mode.

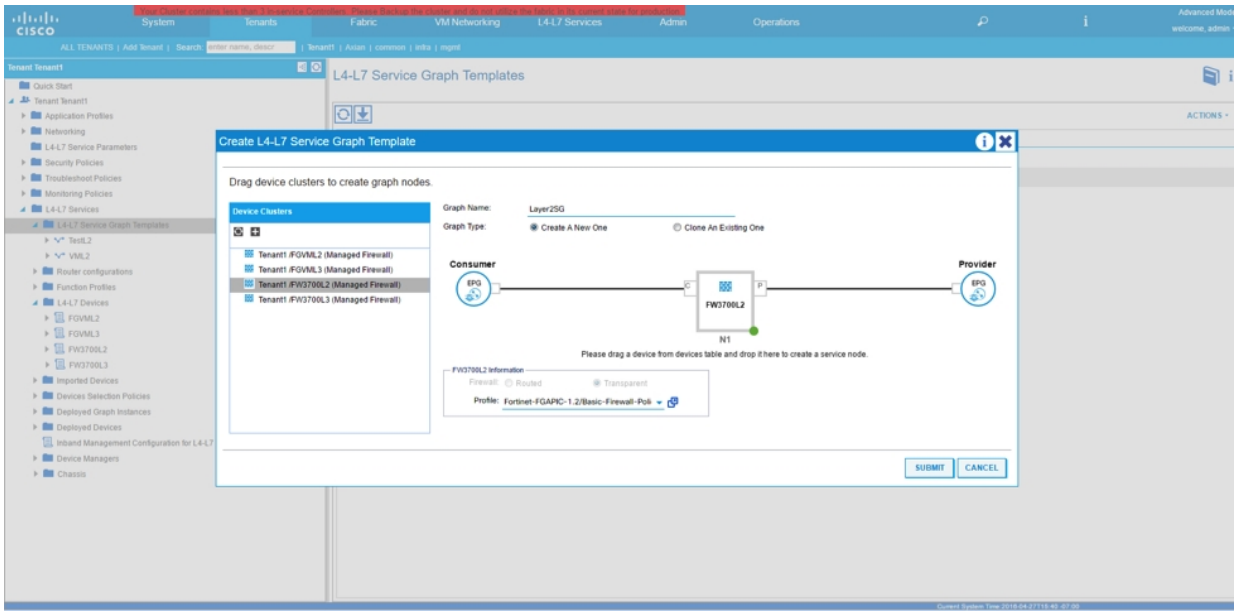
Function Config

Function Config consist of:

- **Network**
  - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
  - This folder is the container for following list of Folders:
    a. FWServiceFolder – Firewall Service Object container
    b. IPv4/IPv6 DoS Policy – Dos Policy configuration
    c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
    d. IPv4 Policy – Firewall Policy Rule container
    e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    f. ScheduleFolder – Schedule container
- **VDOM-Folder**
  - VDOM internal and external interfaces

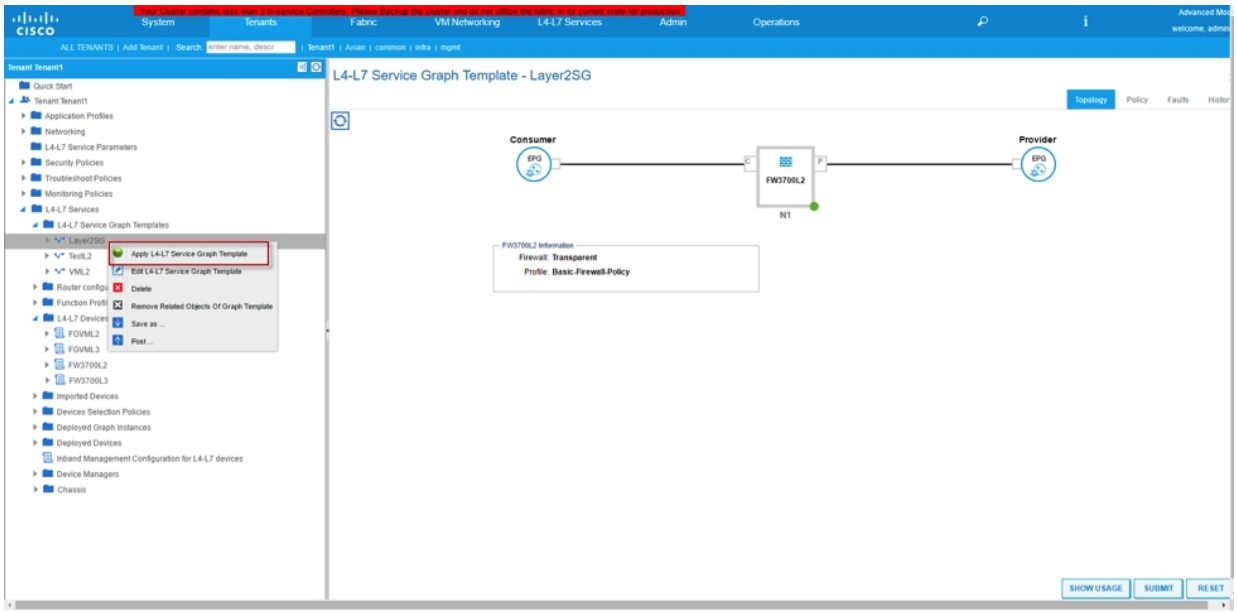
Create Service Graph

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

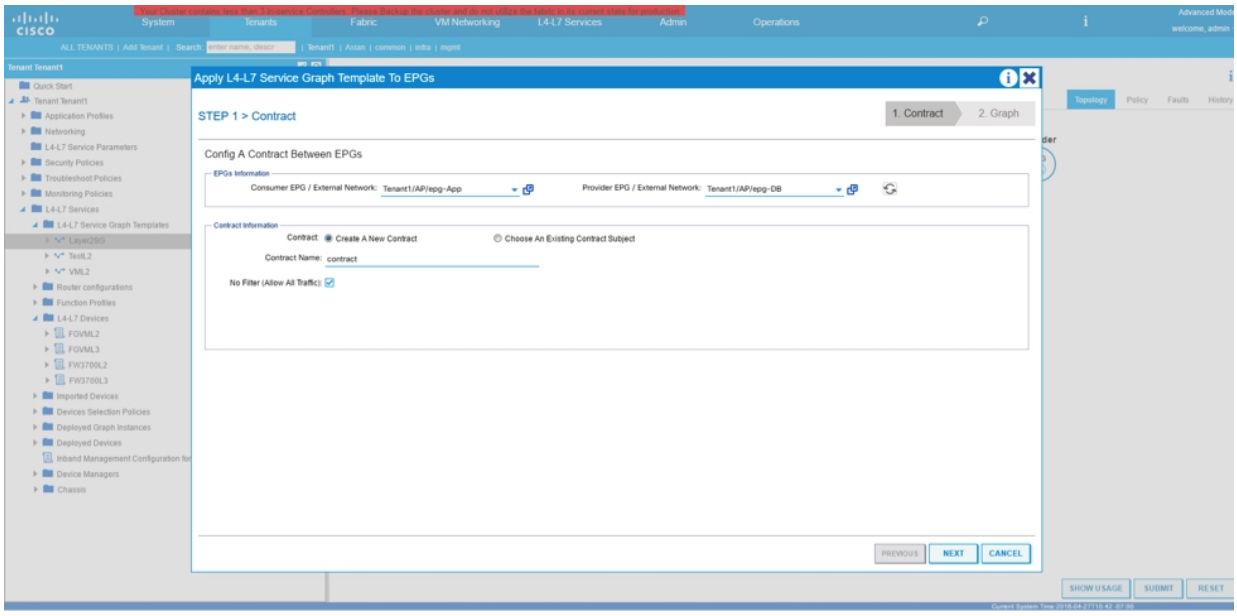


Deploy Service Graph

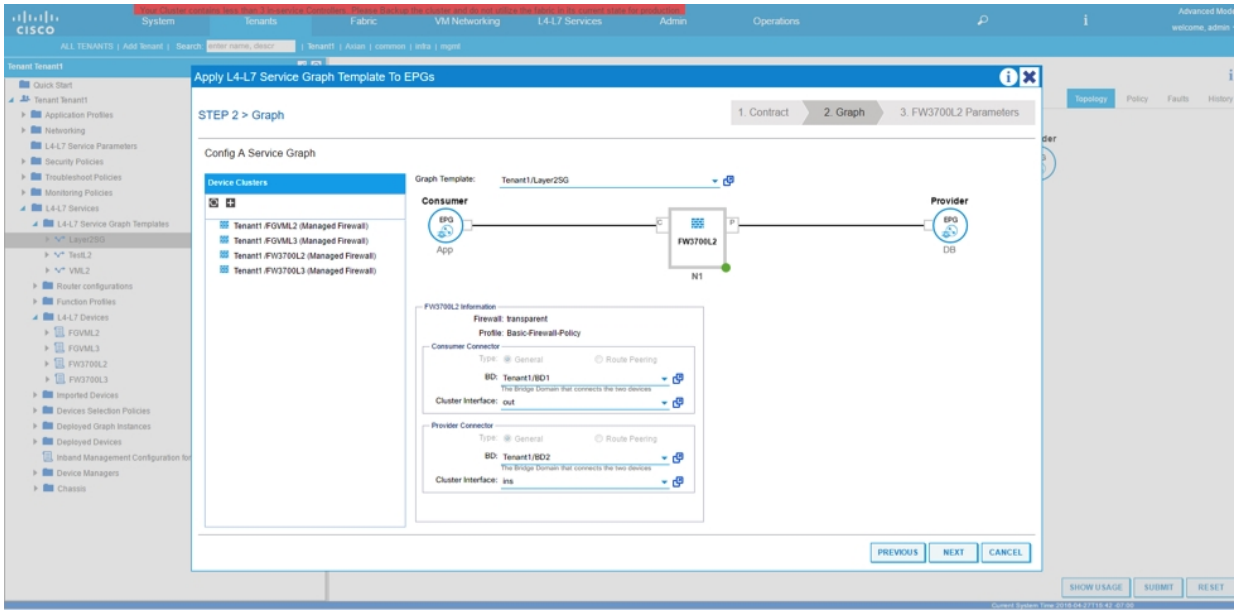
Once we combined the Firewall configuration and associated device together, we are ready to deploy the Service Graph.



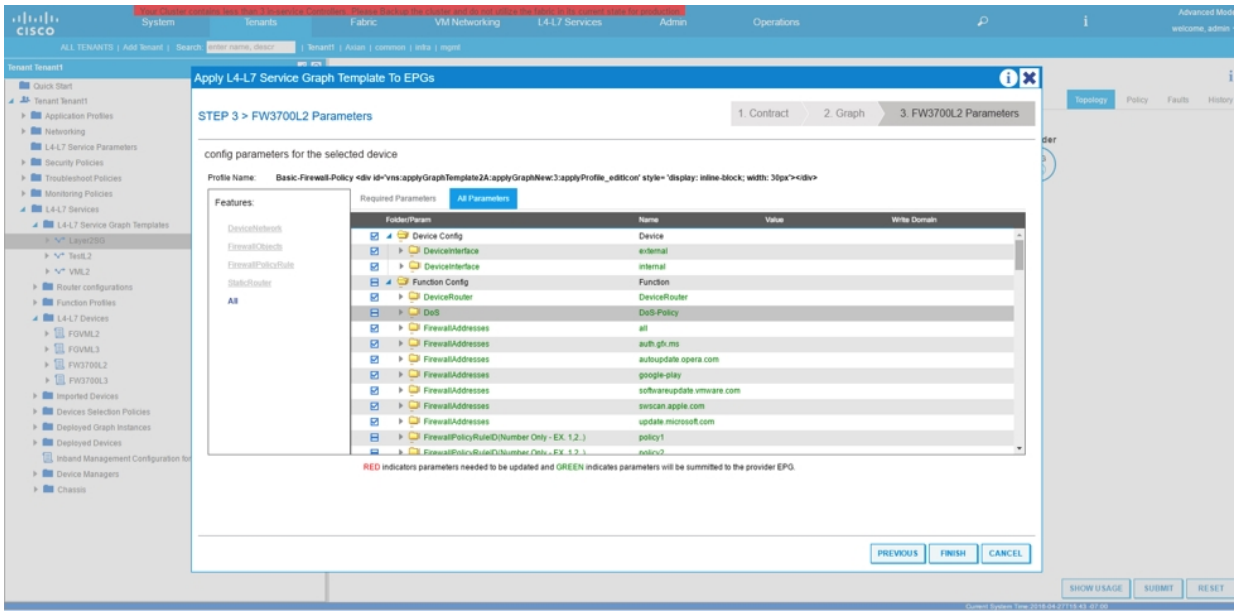
On next screen select the Consumer and Provider EPGs and assign a contract name or select a pre-define contract.



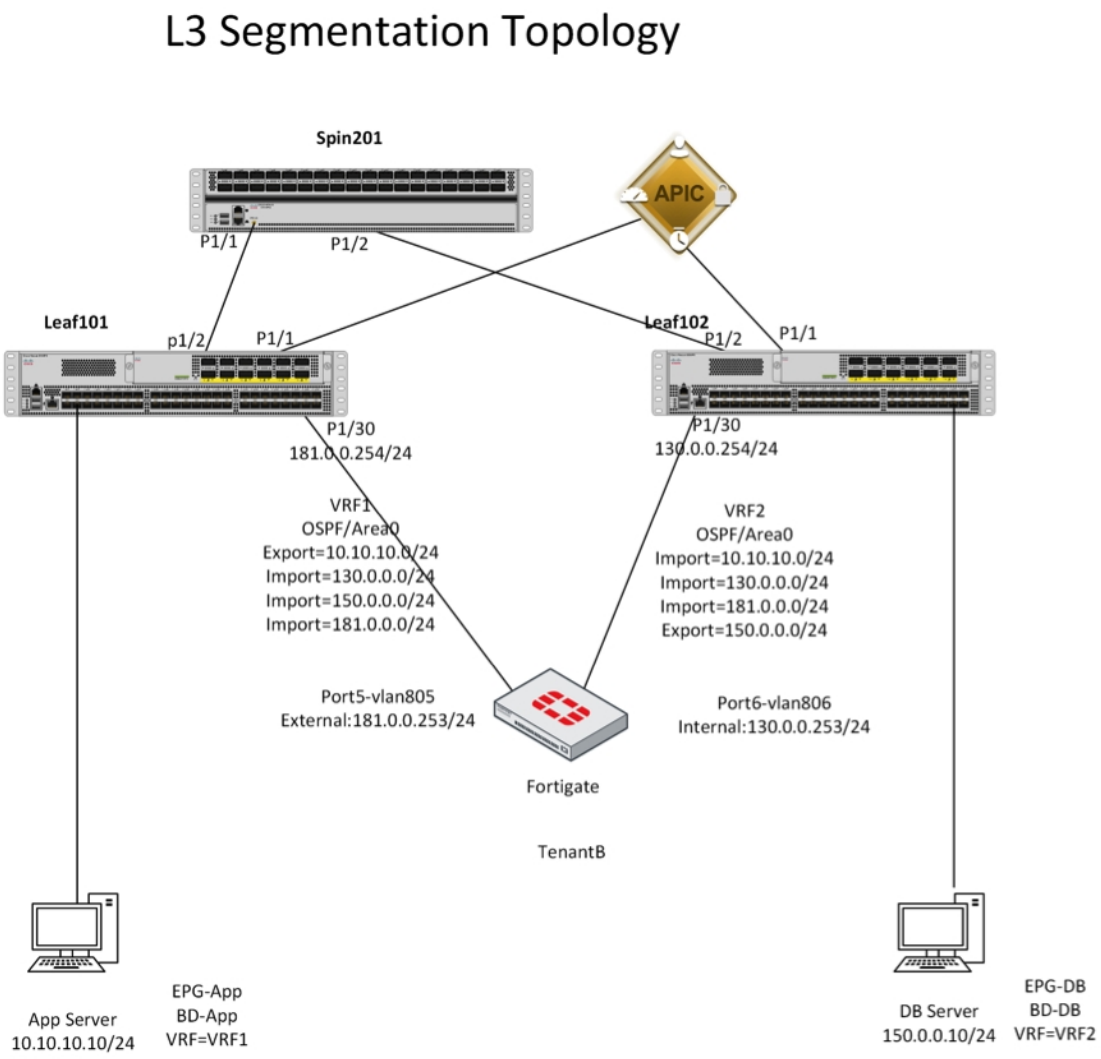
Next screen select the logical interfaces defined during the creation of L4-L7 Device.



Next screen is the last minute to validate all configurations before deploy, then hit the submit button.


Apply L4-L7 Service Graph Template To EPGs
STEP 3 > FW3700L2 Parameters
1. Contract
2. Graph
3. FW3700L2 Parameters
config parameters for the selected device
Profile Name:
Basic-Firewall-Policy
Features:
Required Parameters
All Parameters
Folder/Param
Name
Value
Write Domain
Device Config
Device
DeviceInterface
external
DeviceInterface
internal
Function Config
Function
DeviceRouter
DeviceRouter
DoS
DoS-Policy
FirewallAddresses
all
FirewallAddresses
auth.gfx.ms
FirewallAddresses
autoupdate.opera.com
FirewallAddresses
google-play
FirewallAddresses
softwareupdate.vmware.com
FirewallAddresses
swscan.apple.com
FirewallAddresses
update.microsoft.com
FirewallPolicyRuleID(Number Only - EX. 1,2..)
policy1
RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.
PREVIOUS
FINISH
CANCEL
SHOW USAGE
SUBMIT
RESET

Deploying Data Center Layer 3 Segmentation with Cisco ACI and FortiGate



Introduction

This document describes the configuration walk through of L4-L7 Service Graph with L3 Segmentation within Data Center.

Prerequisites

Please pre-configure below configuration before deploying this design:

- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain

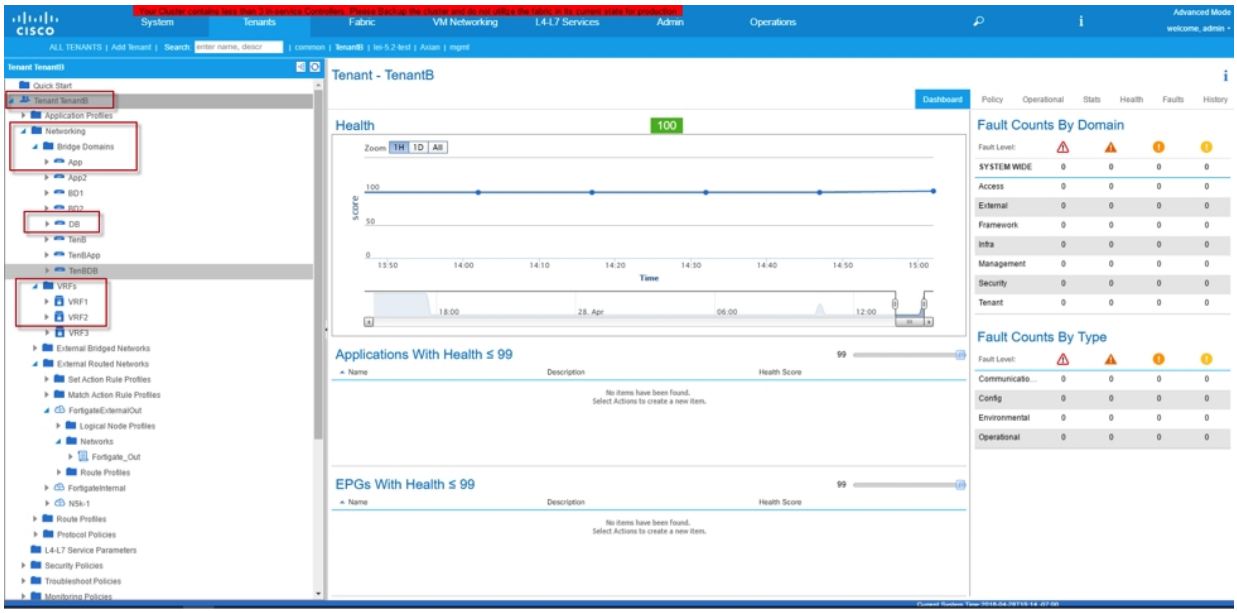
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- L4-L7 Device Package has imported into Cisco APIC

Work Flow

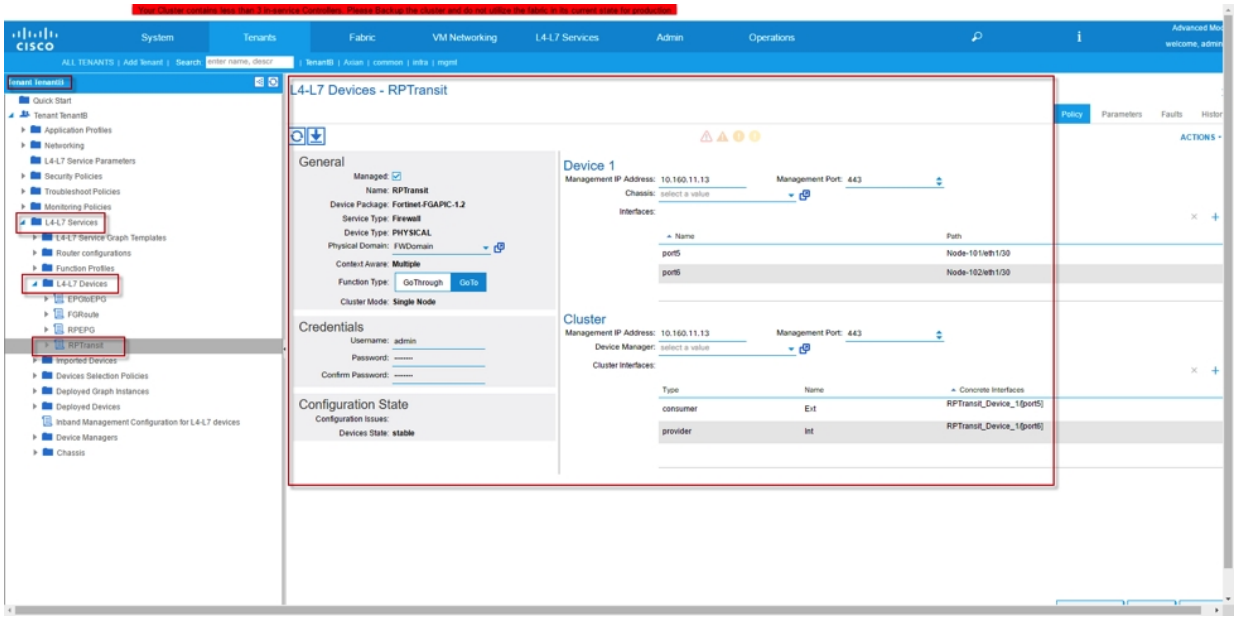
1. Create Tenant (TenantB in our example)
2. Create VRFs (VRF1 and VRF2 in our example)
3. Create Bridge Domains and map to VRFs (Bridge Domain App and DB are mapped to VRF1 and VRF2 respectively in our example)
4. Create EPGs and map to Bridge Domains (EPG-DB and EPG-App in our example)
5. Create two L3Out EPGs (1 for Firewall External and 1 for Firewall Internal. In our example, we created “FortigateExternalOut” for Firewall External and “FortigateInternal” for Firewall Internal)
6. Configure gateway IPs on Bridge Domains (DB and App) for App and DB Servers
7. Ensure “Unicast Routing” is checked in each Bridge Domain
8. In Bridge Domain App, associate L3Outs to “FortigateExternalOut”; in Bridge Domain DB, associate L3Outs to “FortigateInternal”
9. Map App and DB machines to EPGs and configure correct IP addresses, and use Bridge Domain IP address (configured in step 6) as its gateway
10. Verify App and DB machines can ping to gateway IP address
11. Create L4-L7 Device with GoTo mode
12. Create Functional Profile Group as well as Functional Profile
13. Create Route Profiles
14. Create L4-L7 Service Graph Template
15. Deploy L4-L7 Service Graph

Configuration

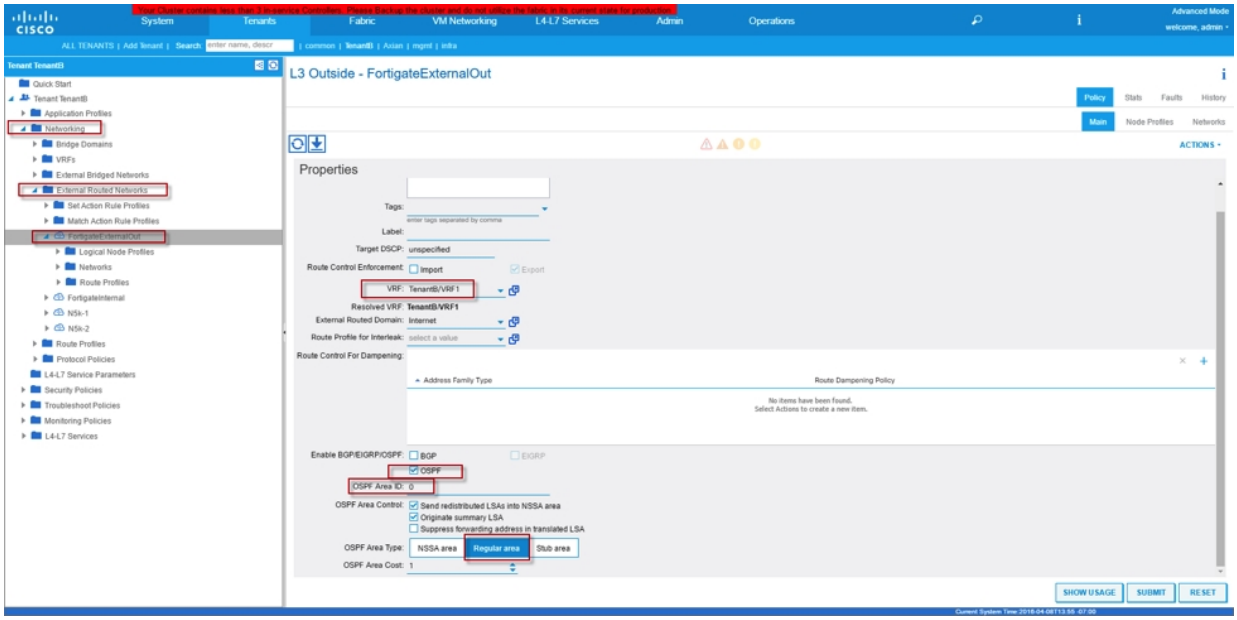
Configure the Bridge Domain DB and App as well as VRF1 and VRF2. Associate Bridge Domain App to VRF1 and Bridge Domain DB to VRF2.



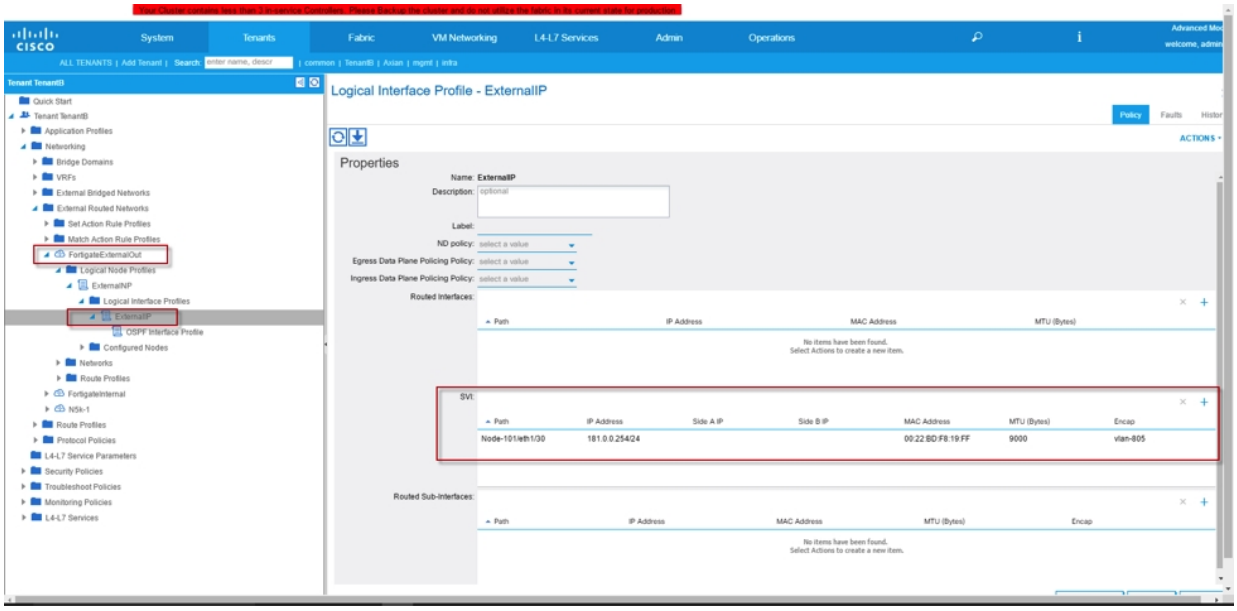
Configure L4-L7 Device for physical Fortigate (GoTo Mode)



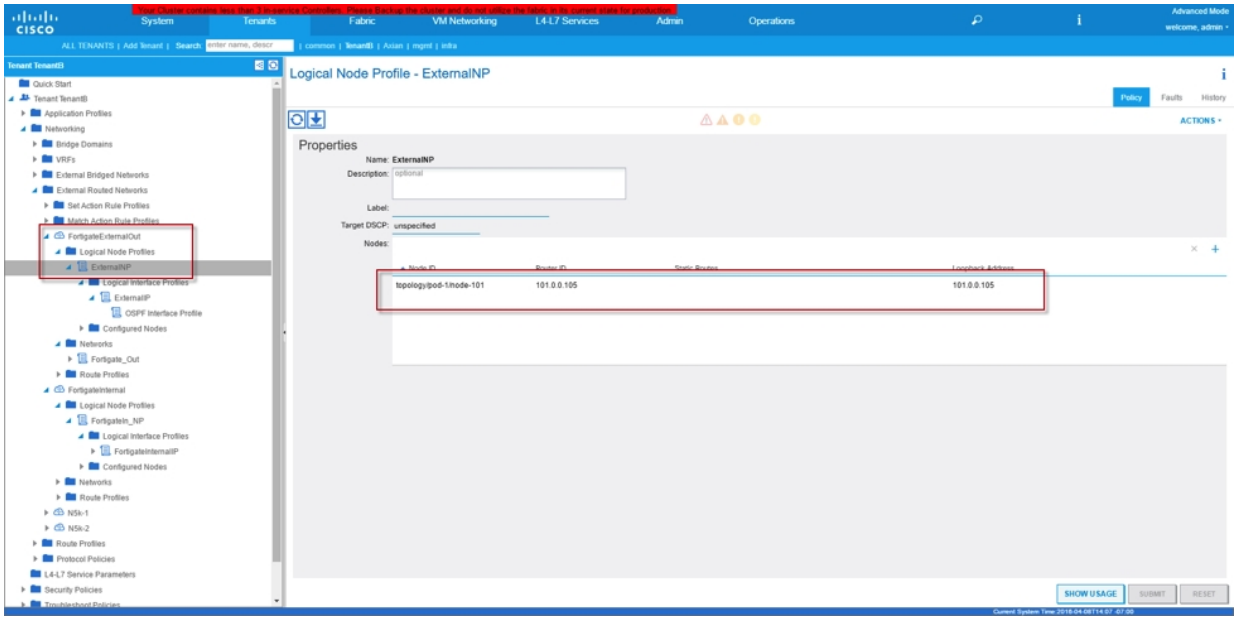
Configure L3Out for Fortigate External Interface and associate with VRF1



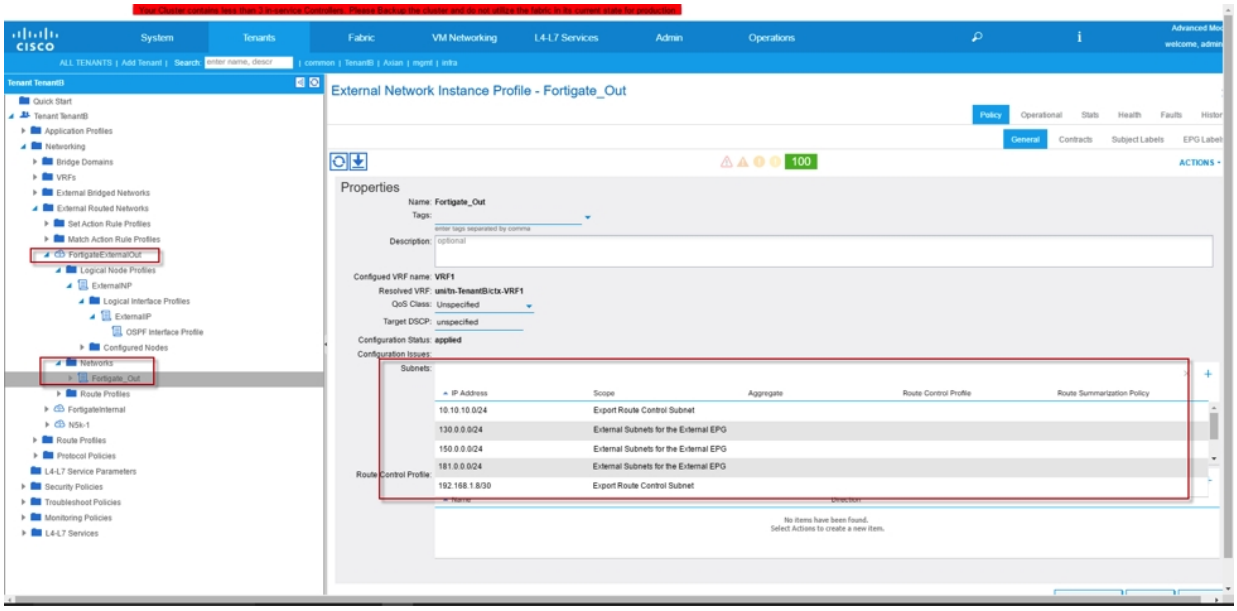
Configure SVI for L3Out Fortigate External out



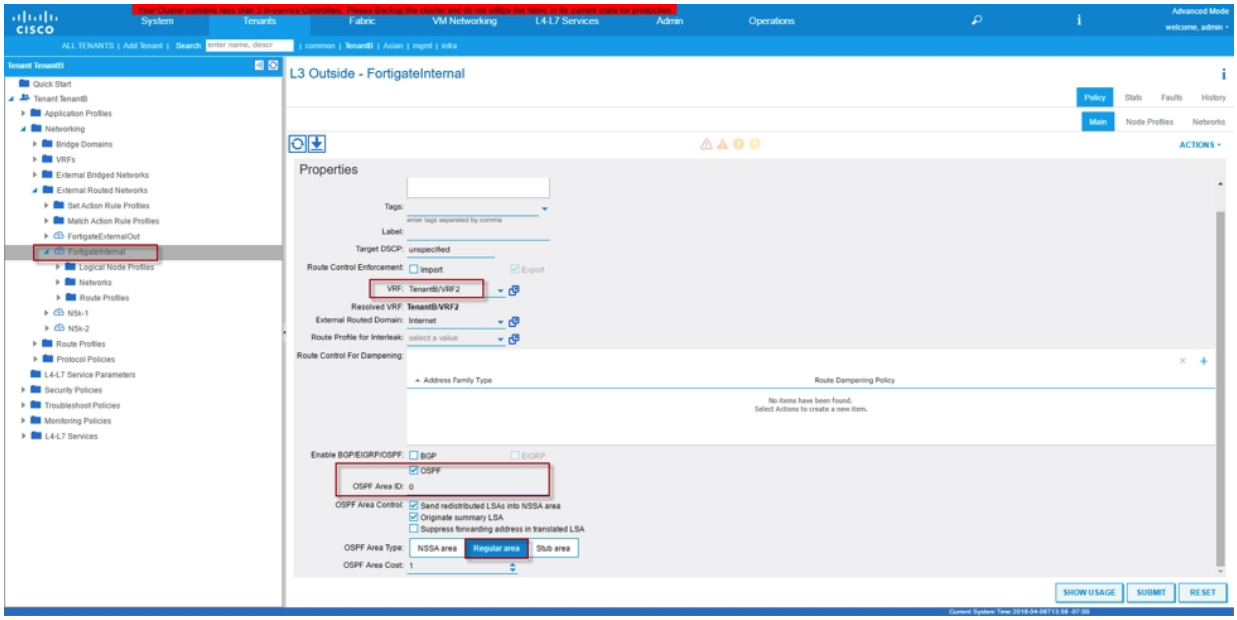
Configure Route ID for L3Out Fortigate External Out



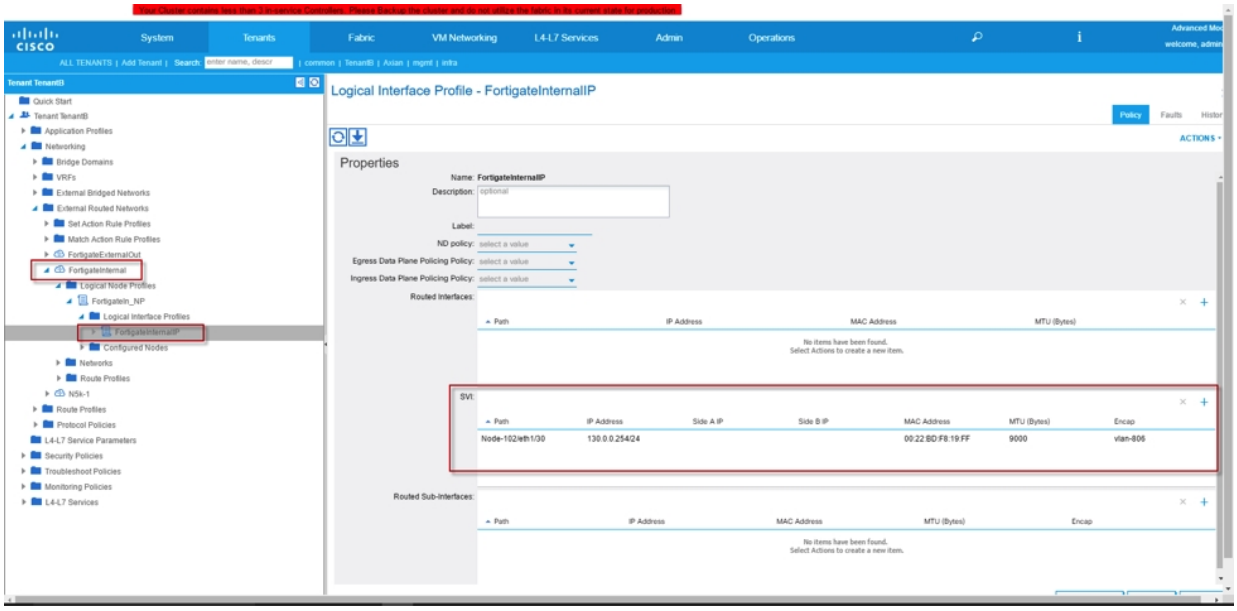
Configure Import/Export Route Control on Subnets for Fortigate External out



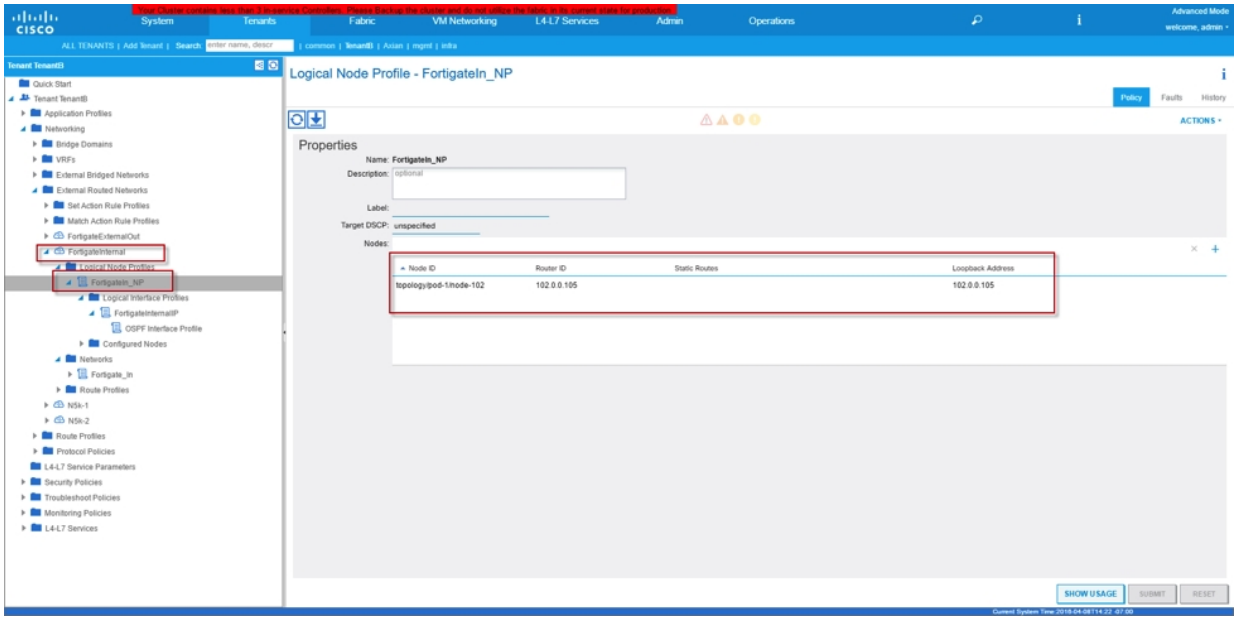
Configure L3Out for Fortigate Internal and associate with VRF2



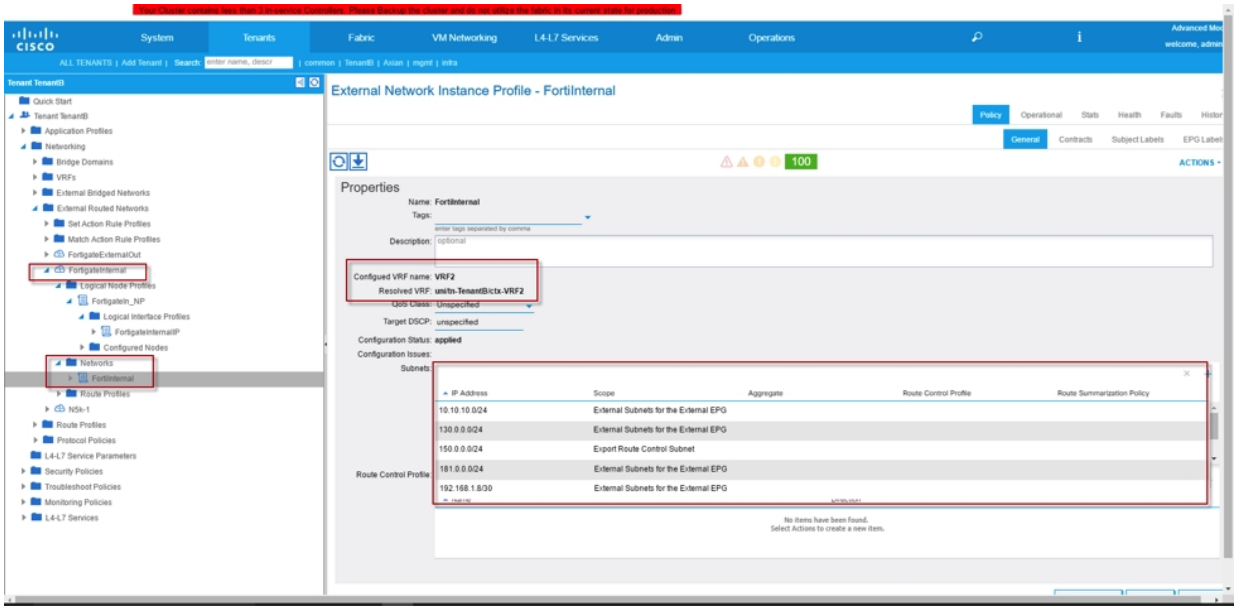
Configure SVI for L3Out Fortigate Internal



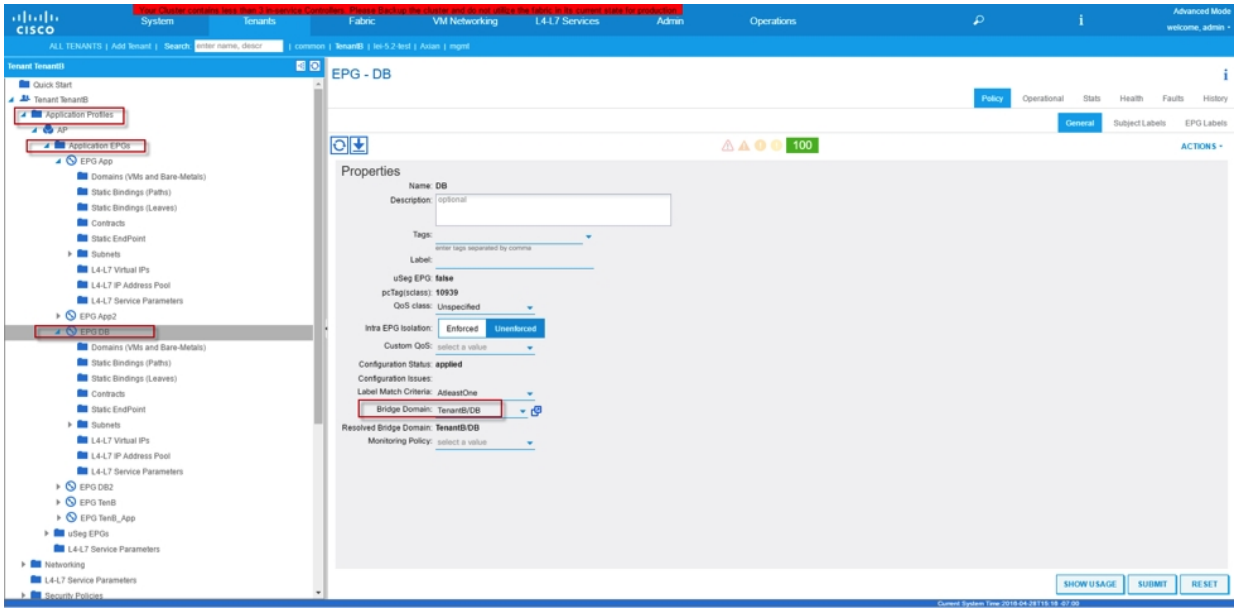
Configure Route ID for L3Out Fortigate Internal

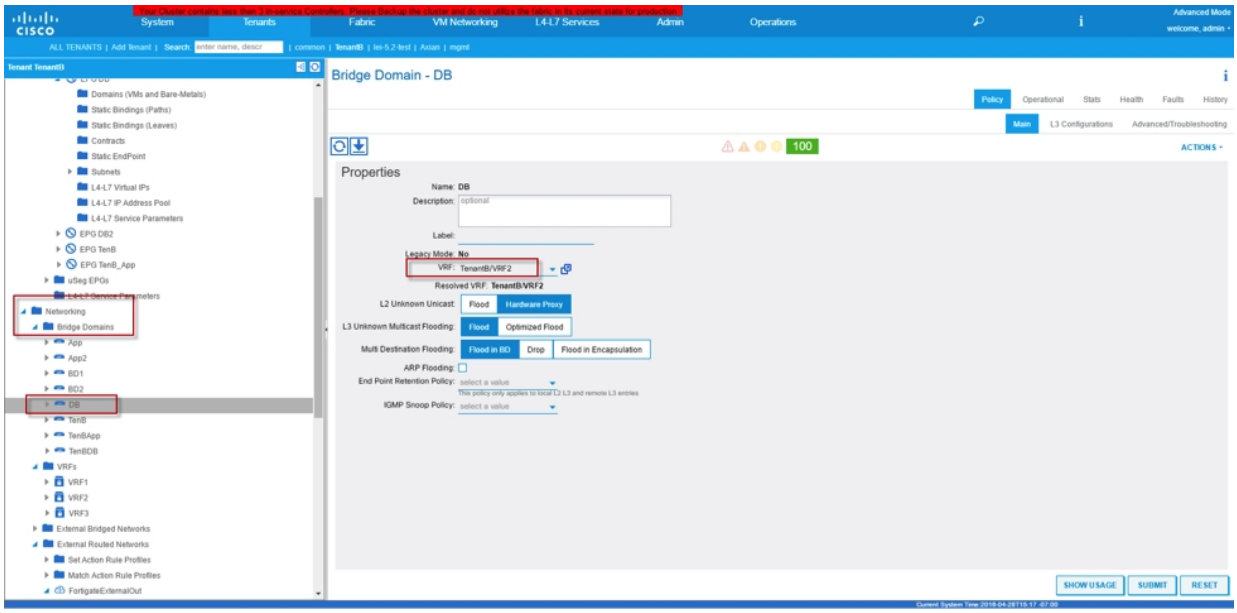


Configure Import/Export Route Control on Subnet for L3Out Fortigate Internal

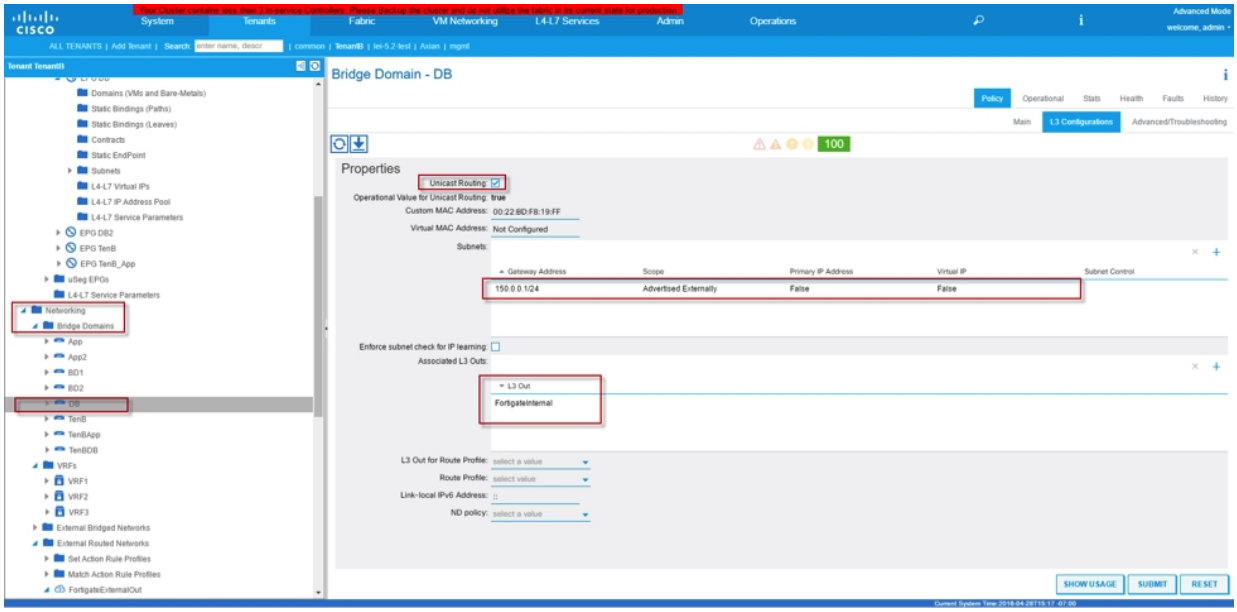


Associate EPG “DB” to Bridge Domain “DB” and attach Bridge Domain to VRF2

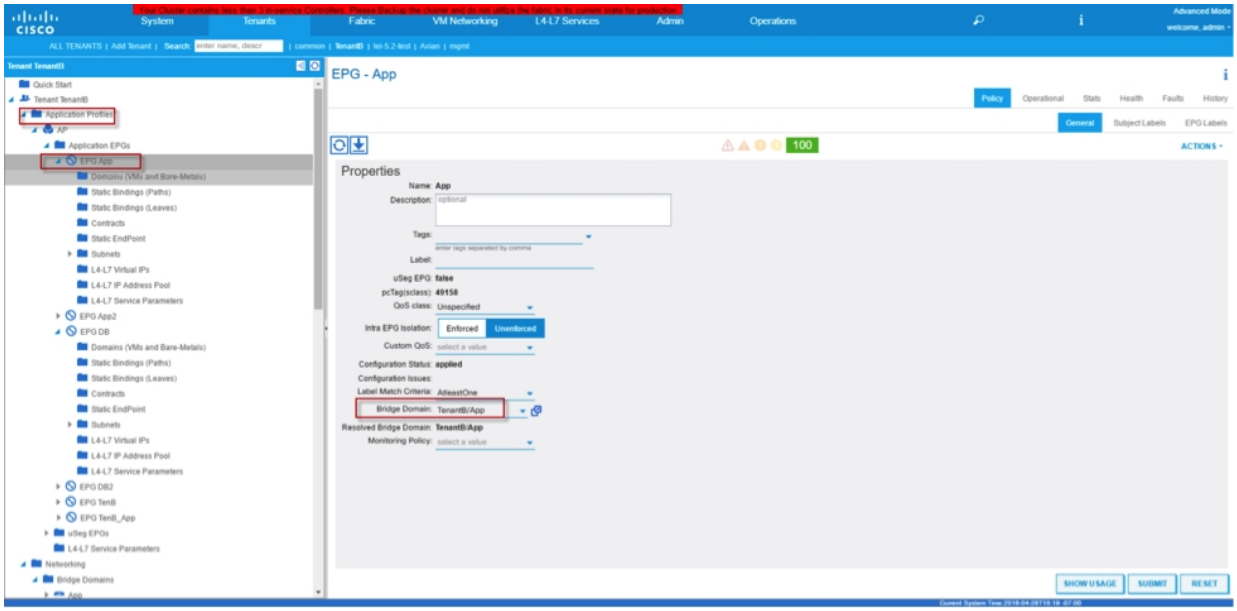


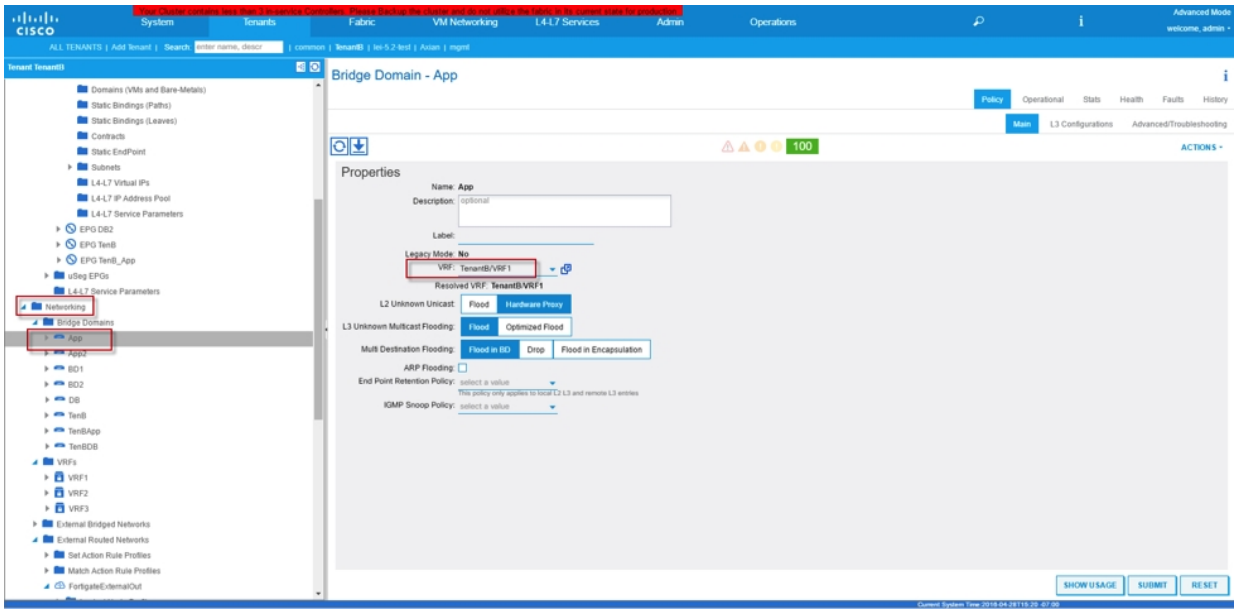


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Out to "FortigateInternal"

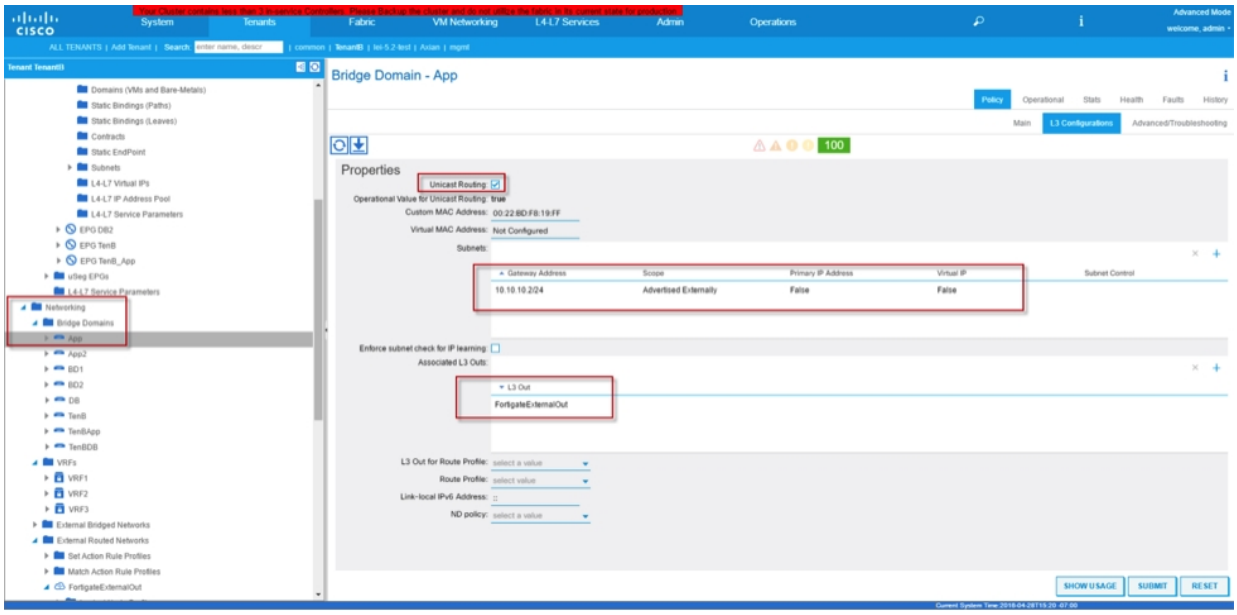


Associate EPG "App" to Bridge Domain "App" and attach Bridge Domain to VRF1

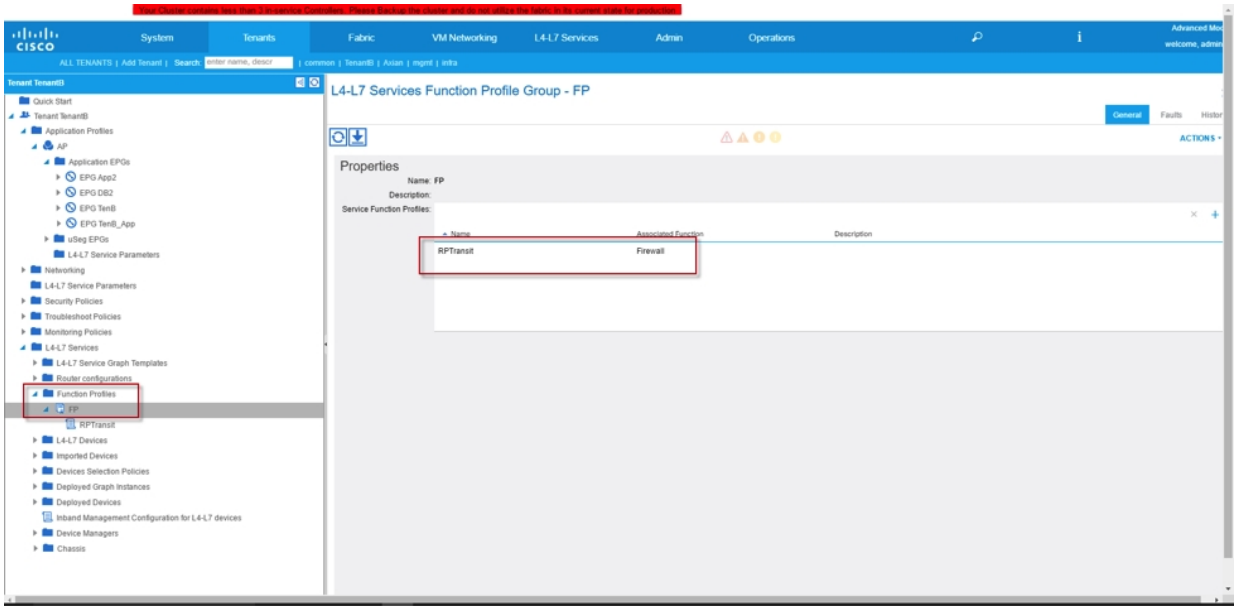


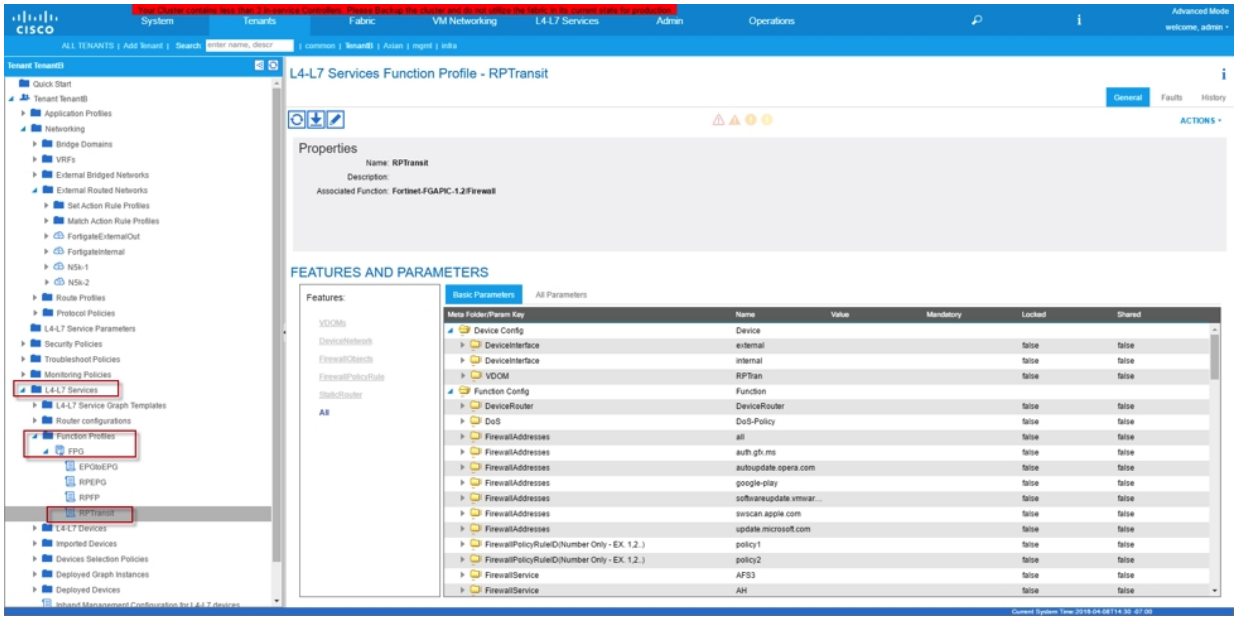


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Out to “FortigateInternal”

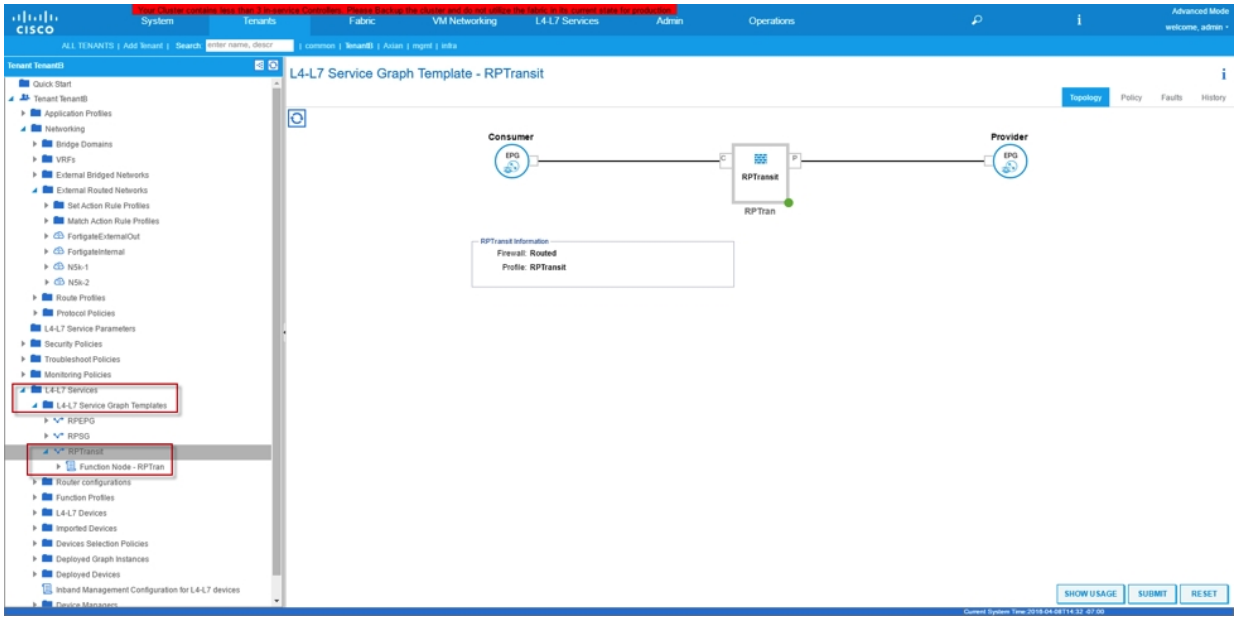


Create Functional Profile Group and Functional Profile from existing template

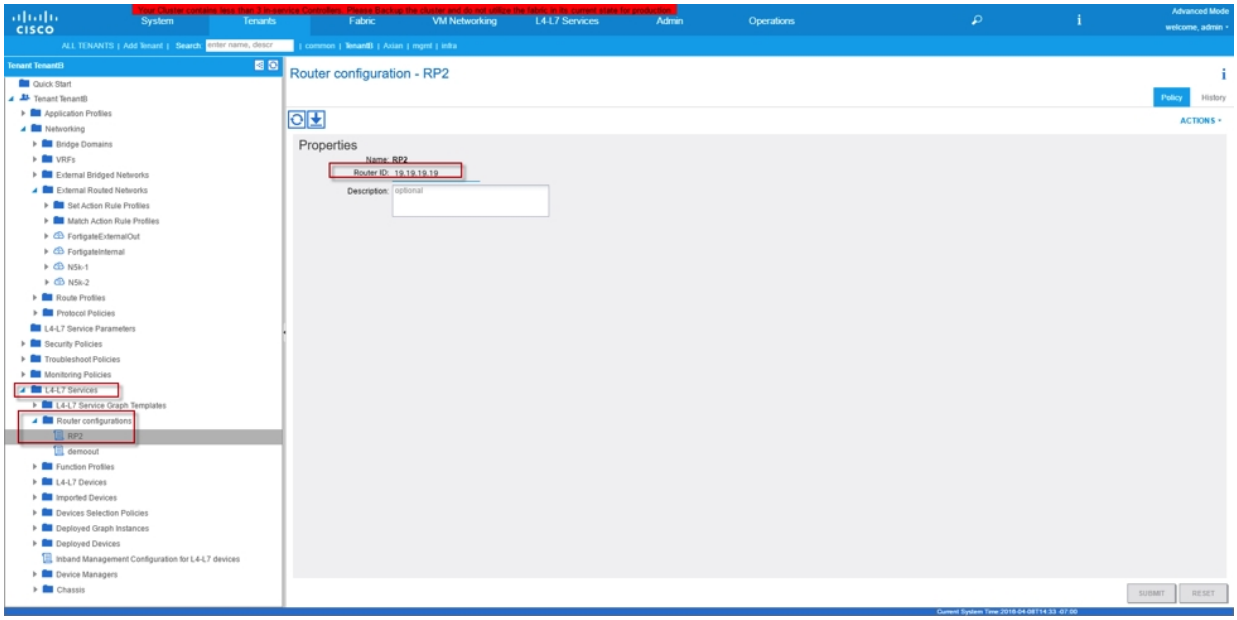




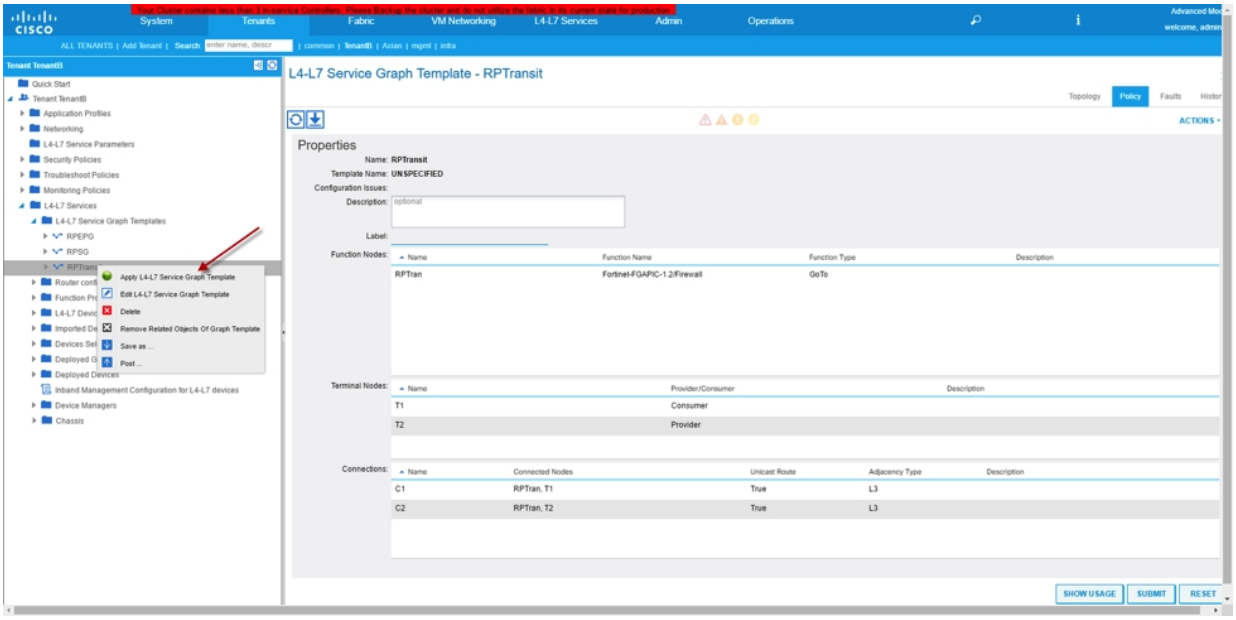
Create Service Graph template



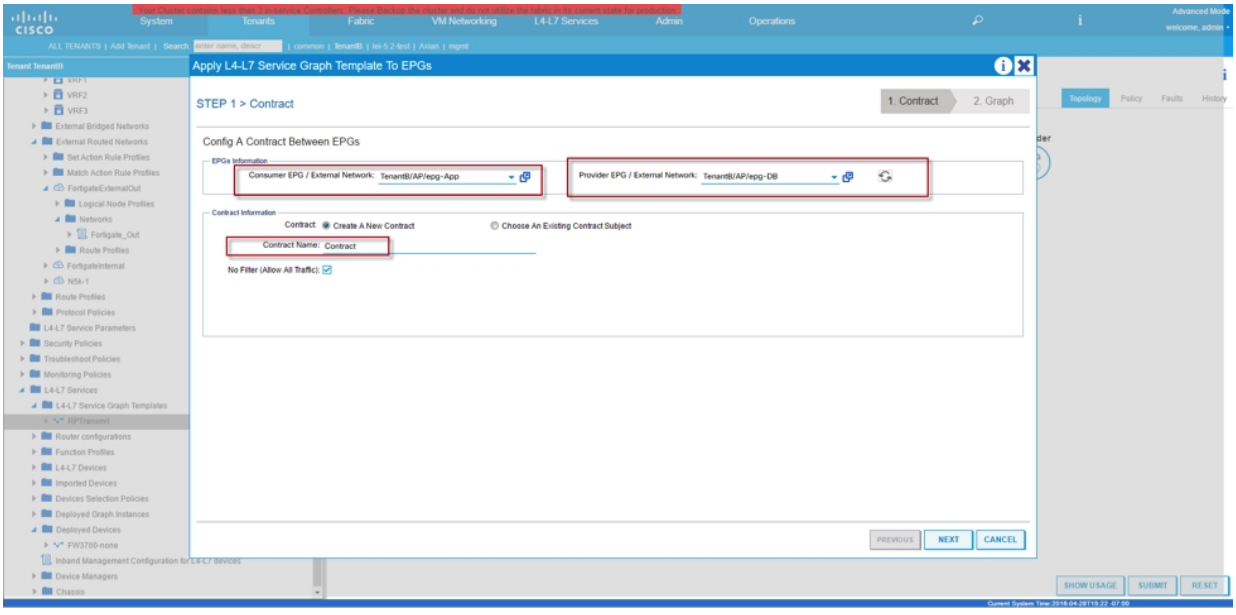
Create Router ID that will be used on the Service Appliance (FortiGate)



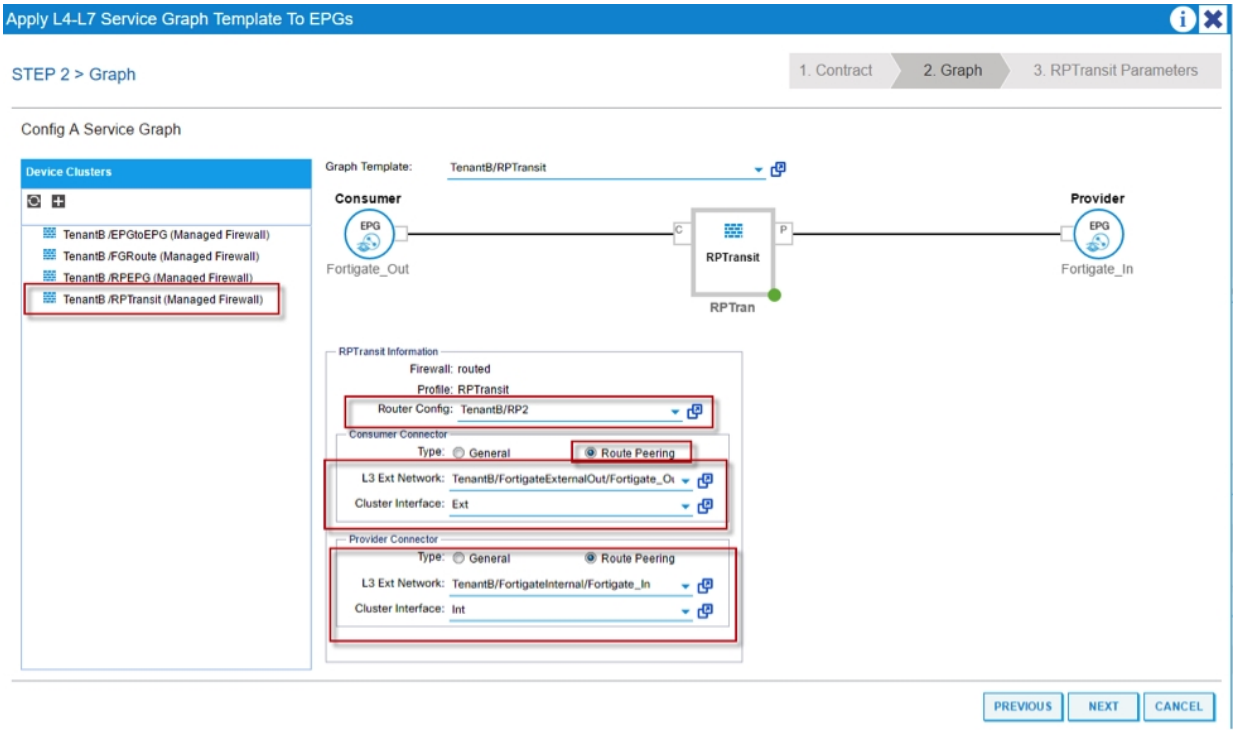
Deploy Service Graph



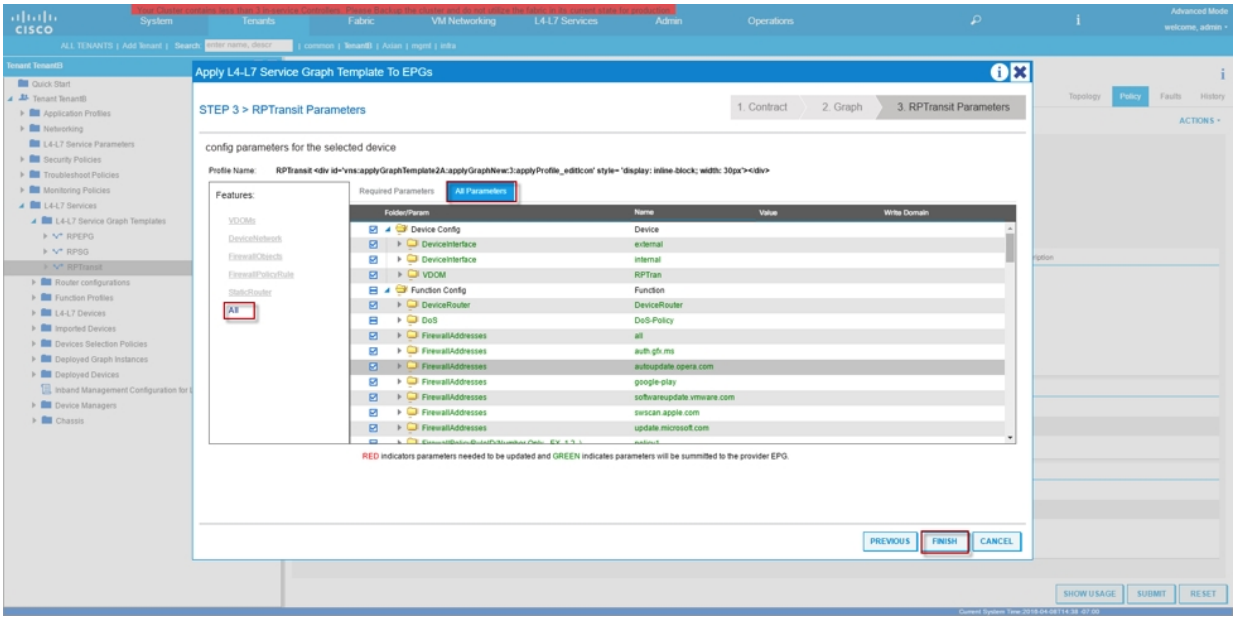
Consumer will be App EPG. Provider is the DB EPG.



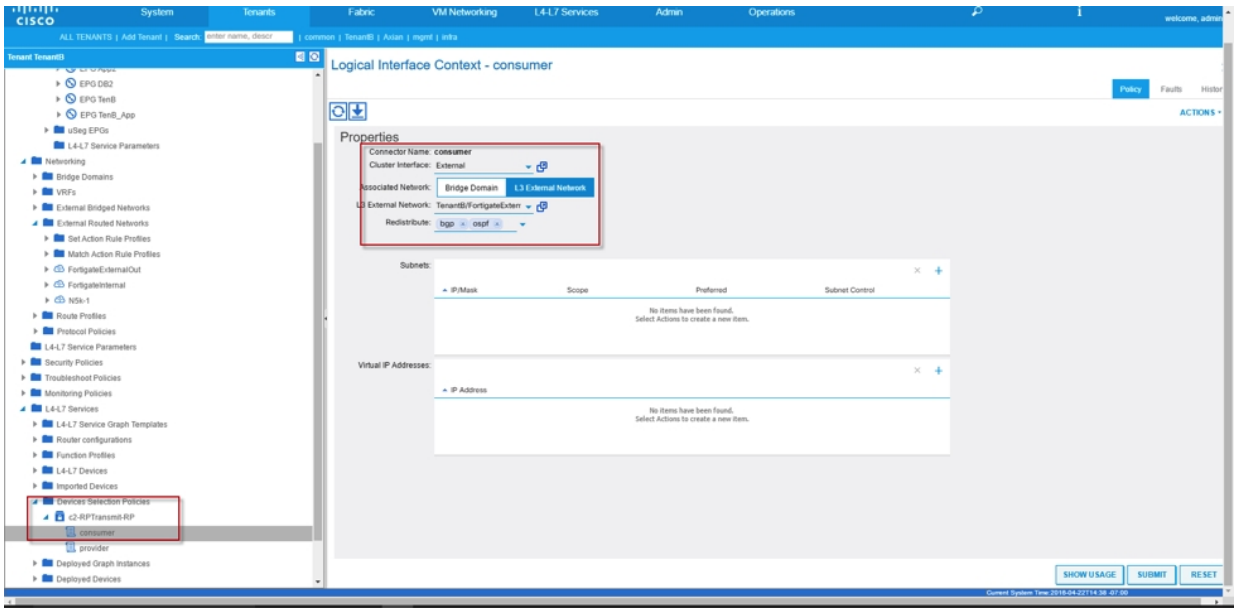
Please select for Internal and external connections. In our example, we used “FortigateExternalOut” and FortigateInternal” as External and Internal selections respectively.

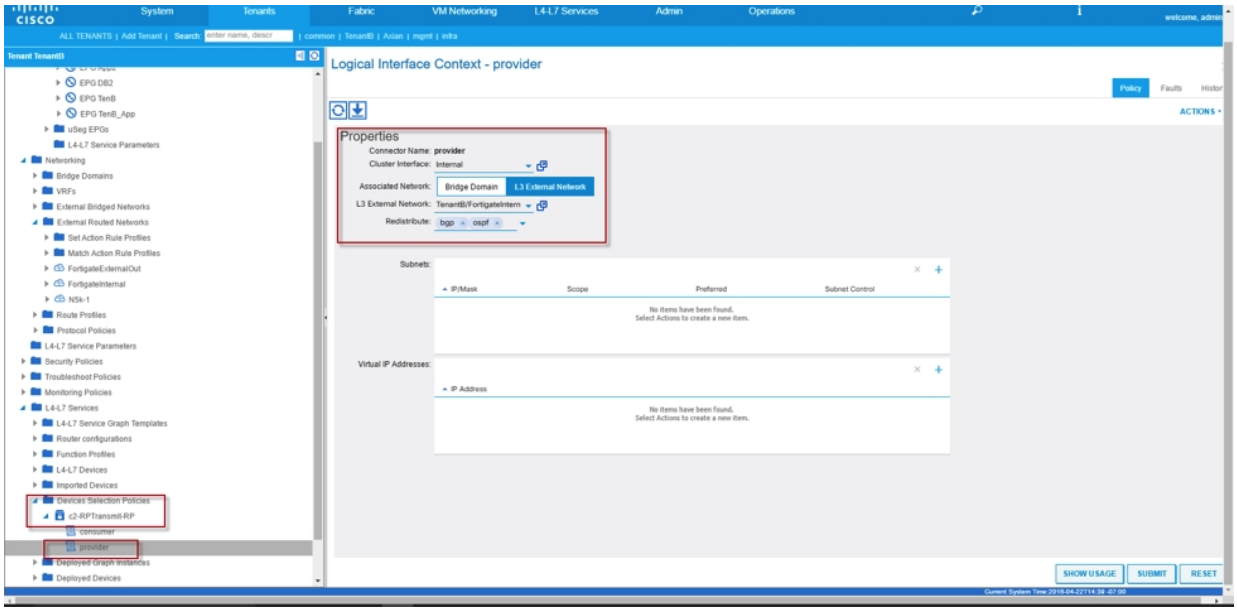


Last minute check to make sure configuration is good before hit “Finish” button

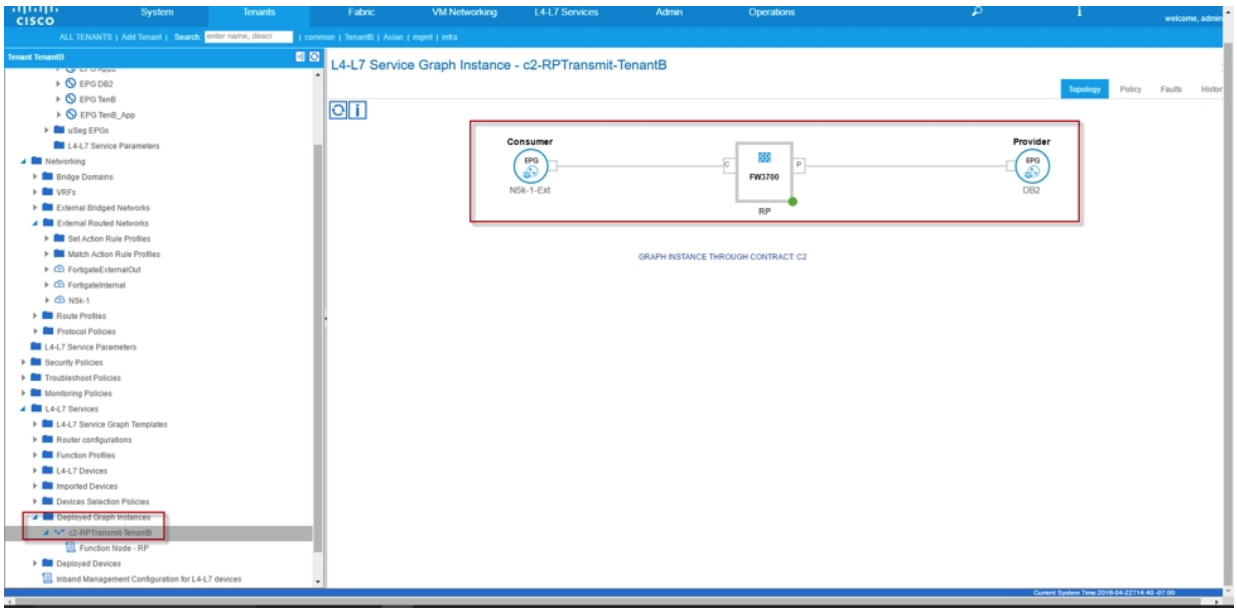


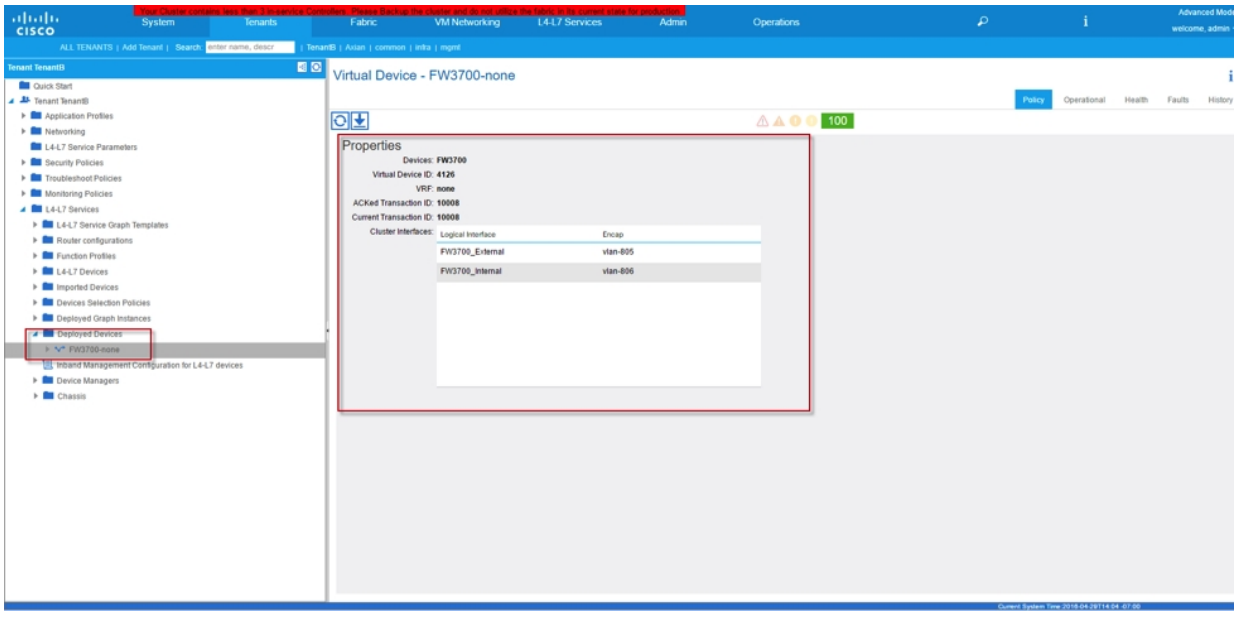
Check the status and verify Device Selection Policy



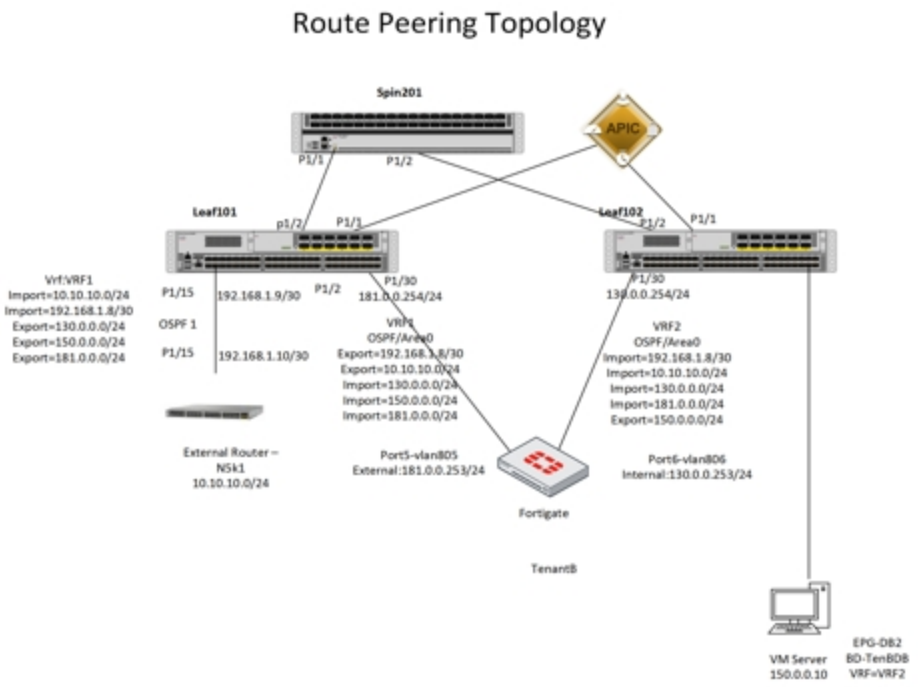


Verify deployed Graph Instance





Deploying Firewall Service for North-to-South traffic with OSPF



Introduction

This document describes the configuration walkthrough of L4-L7 Service Graph with Route Peering, where the consumer is external to ACI Fabric and the provider is internal to the Cisco ACI Fabric. With route peering feature provided by Cisco APIC, external traffic can reach internal servers through L4-L7 Services.

Prerequisites

Please pre-configure below configuration before deploying this design:

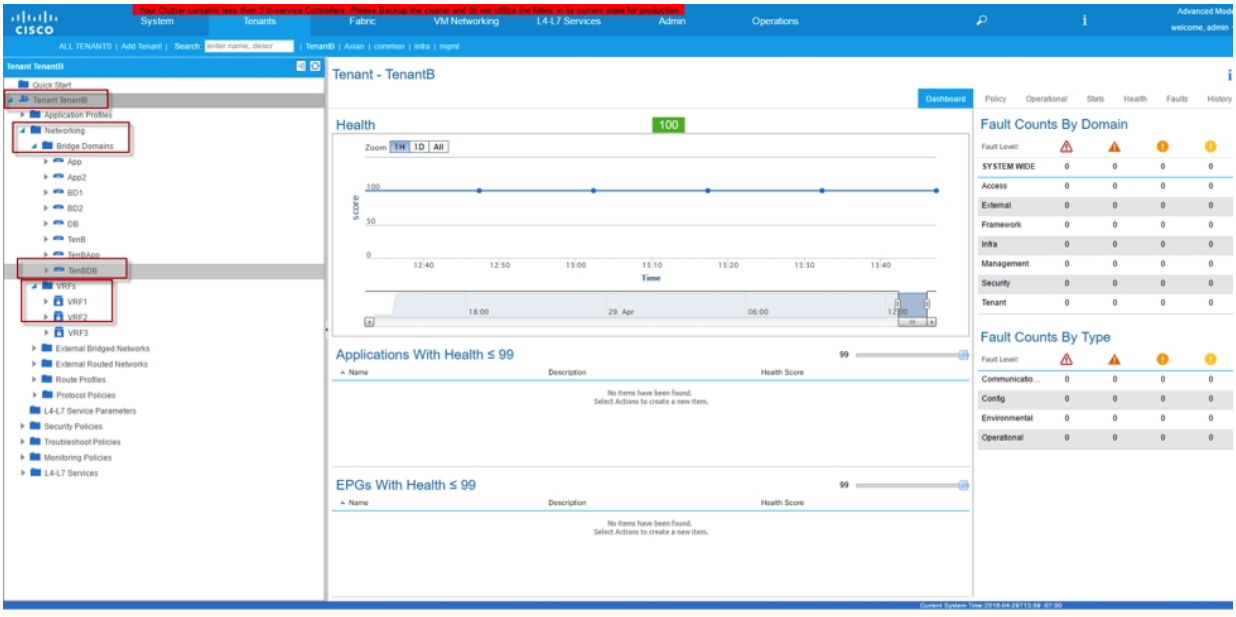
- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- Layer3 Connection Outside of ACI Fabric
- L4-L7 Device Package has imported into Cisco APIC

Work Flow

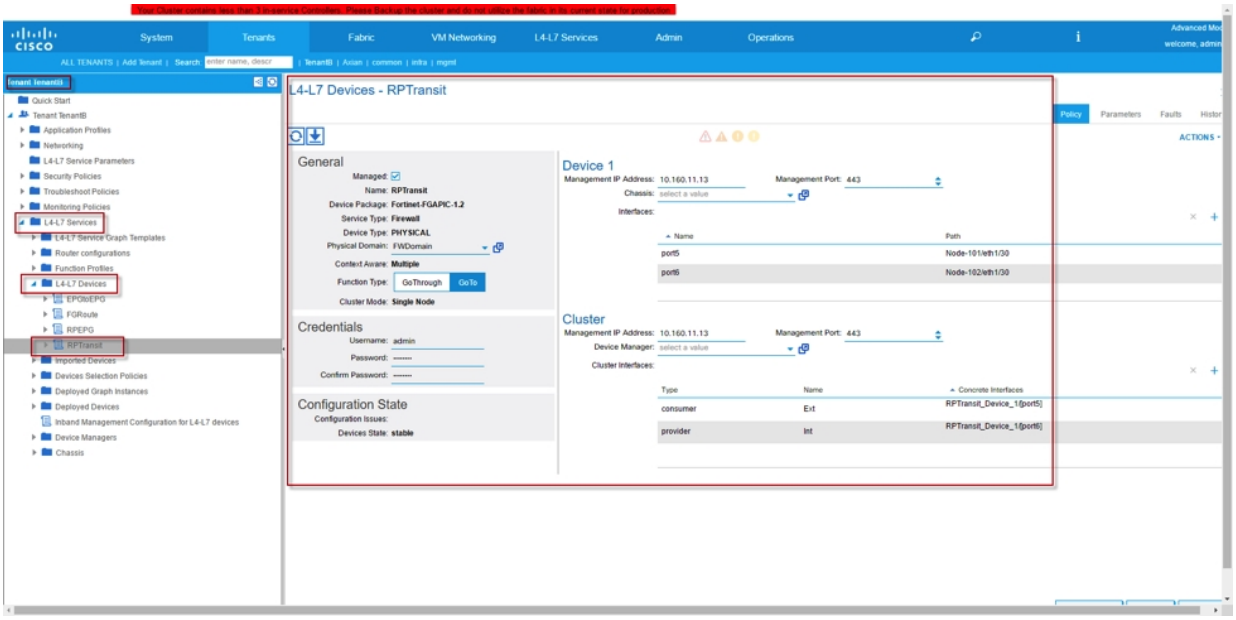
1. Configure routing configuration on external router that attached to ACI Fabric
2. Create Tenant (TenantB in our example)
3. Create VRFs (VRF1 and VRF2 in our example)
4. Create Bridge Domain and map to VRF2 (TenBDB in our example)
5. Create EPG “EPG-DB2” and map it to Bridge Domain “TenBDB”
6. Create three L3Out EPGs (1 for external Connection, 1 for Firewall External and 1 for Firewall Internal. In our example, we used “N5k-1” for external Connection, “FortigateExternalOut” for Firewall External and “FortigateInternal” for Firewall Internal)
7. Create gateway IP on Bridge Domain (TenBDB) for VM Server
8. Ensure “Unicast Routing” is checked on Bridge Domain “TenBDB”
9. In Bridge Domain “TenBDB”, associate L3Outs to “FortigateInternal”
10. Map VM Server to EPG “EPG-DB2” and configure IP address and gateway ip address (TenBDB ip address)
11. Verify VM Server can ping to gateway IP
12. Create L4-L7 Device
13. Create Functional Profile Group as well as Functional Profile
14. Create Route Profiles
15. Create L4-L7 Service Graph Template
16. Deploy L4-L7 Service Graph

Configuration

Configure the Bridge Domain TenBDB, VRF1 and VRF2. Associate Bridge Domain TenBDB to VRF2

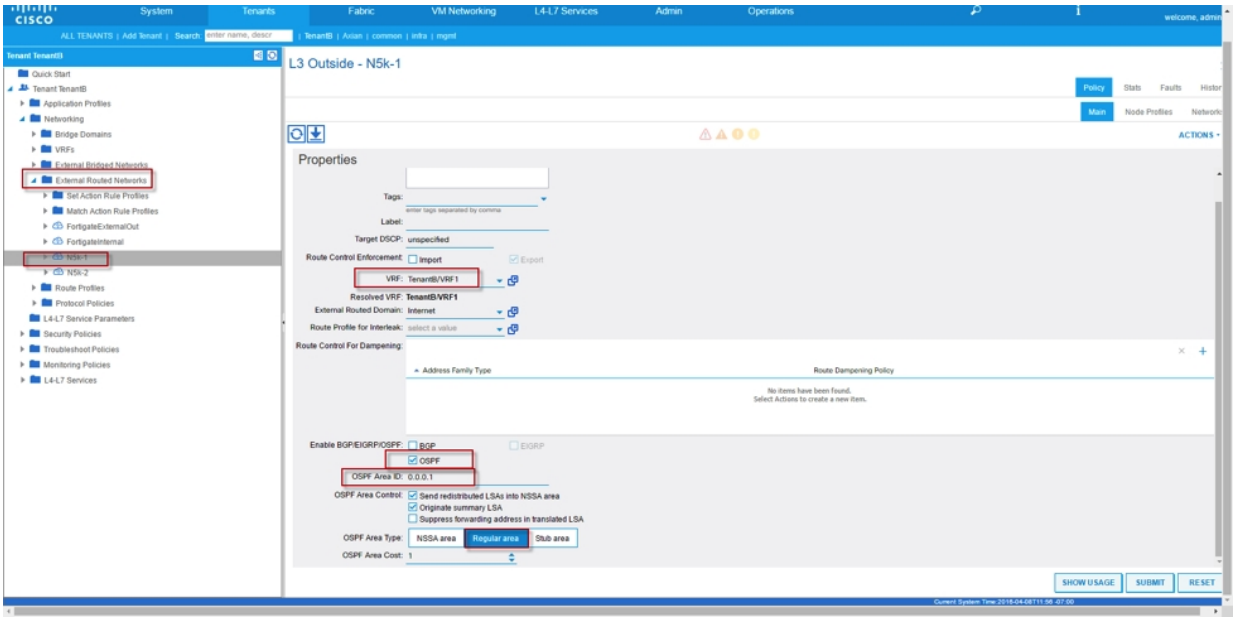


Configure L4-L7 Device for physical Fortigate (GoTo Mode)

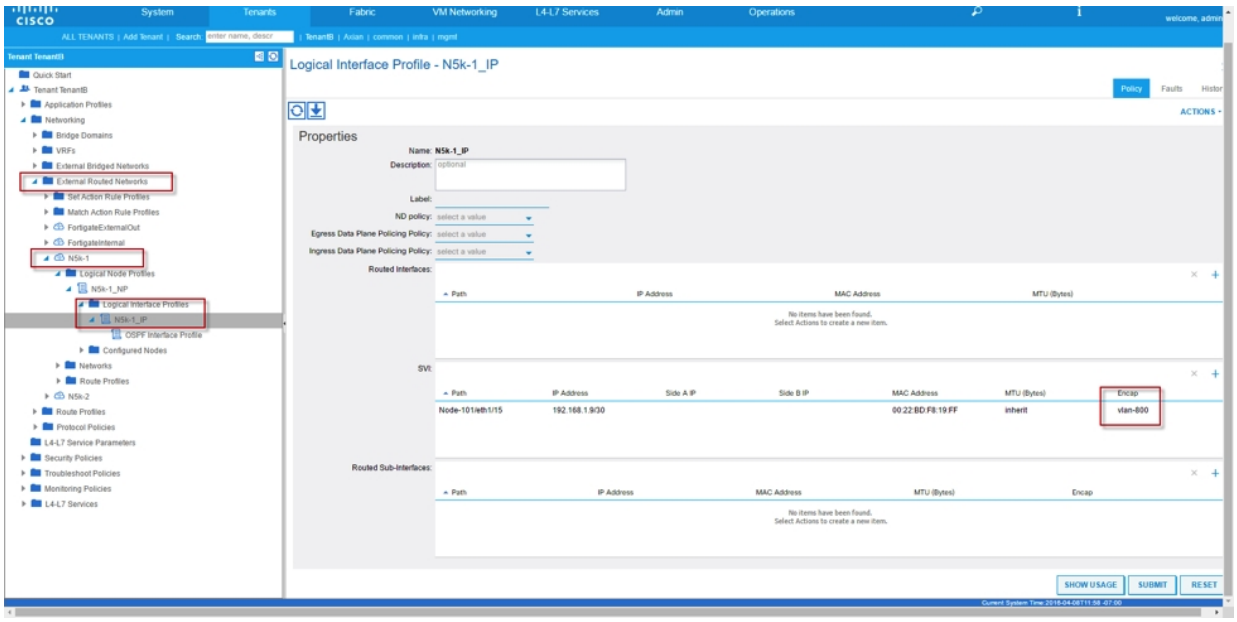


Configure L3Out for N5K-1 and associate to VRF1

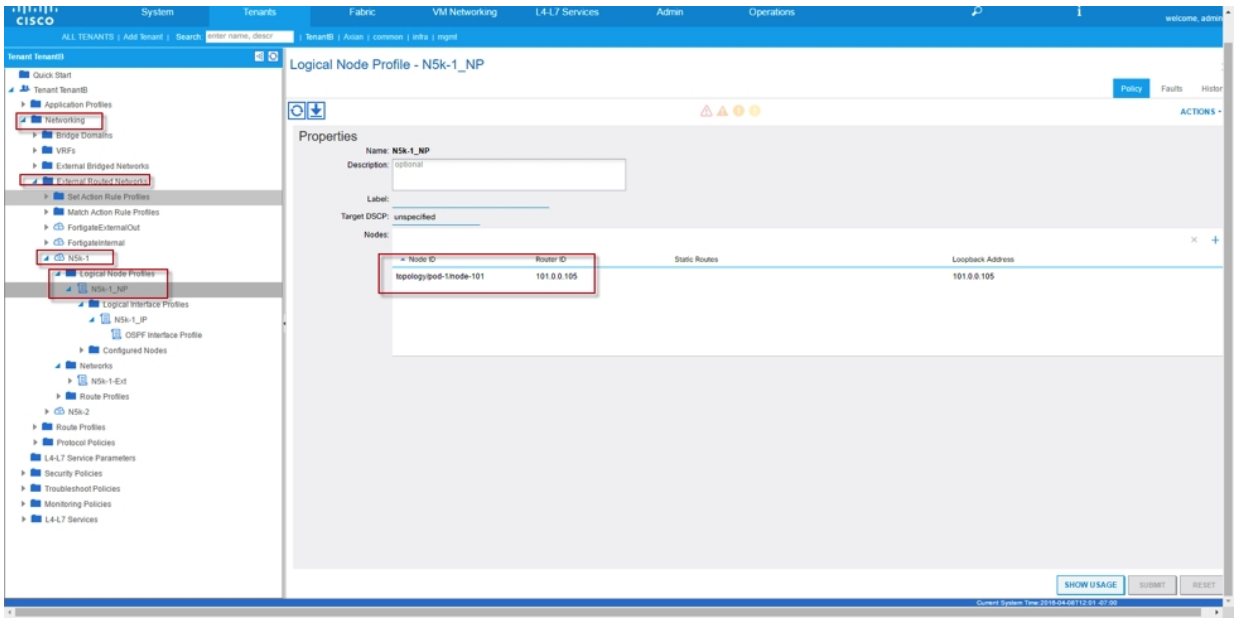
All L3Out Interfaces which are used for Route Peering are required to be configured as a SVI with Vlan Encapsulation accordingly.



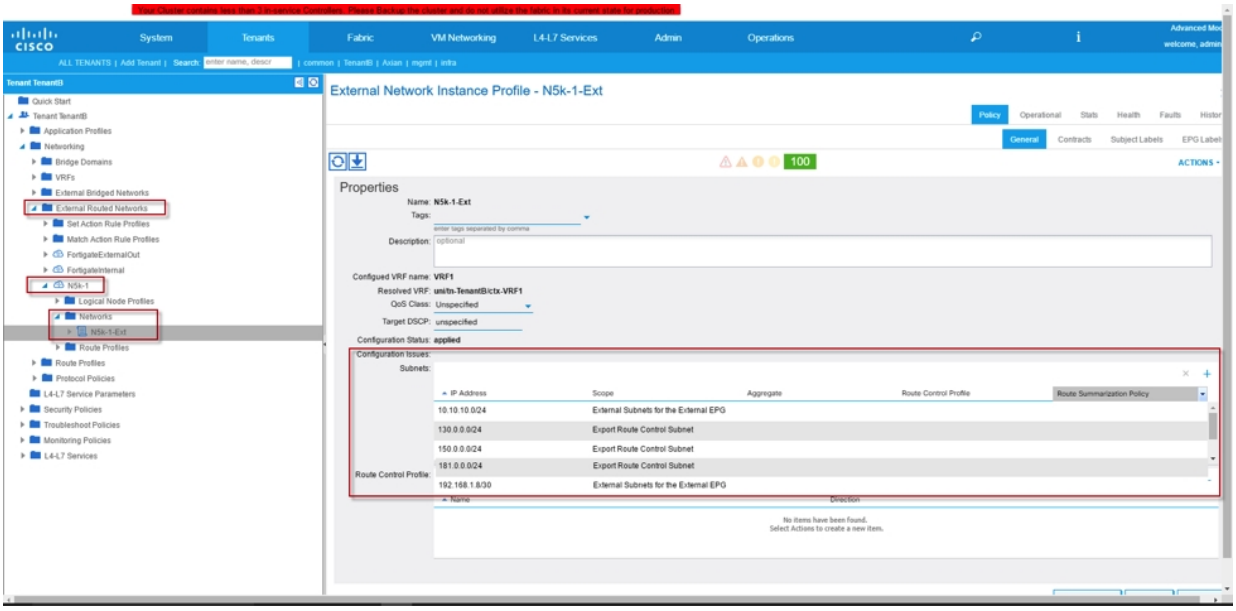
Configure SVI for L3Out N5k-1



Configure Route ID (101.0.0.105 in our example)

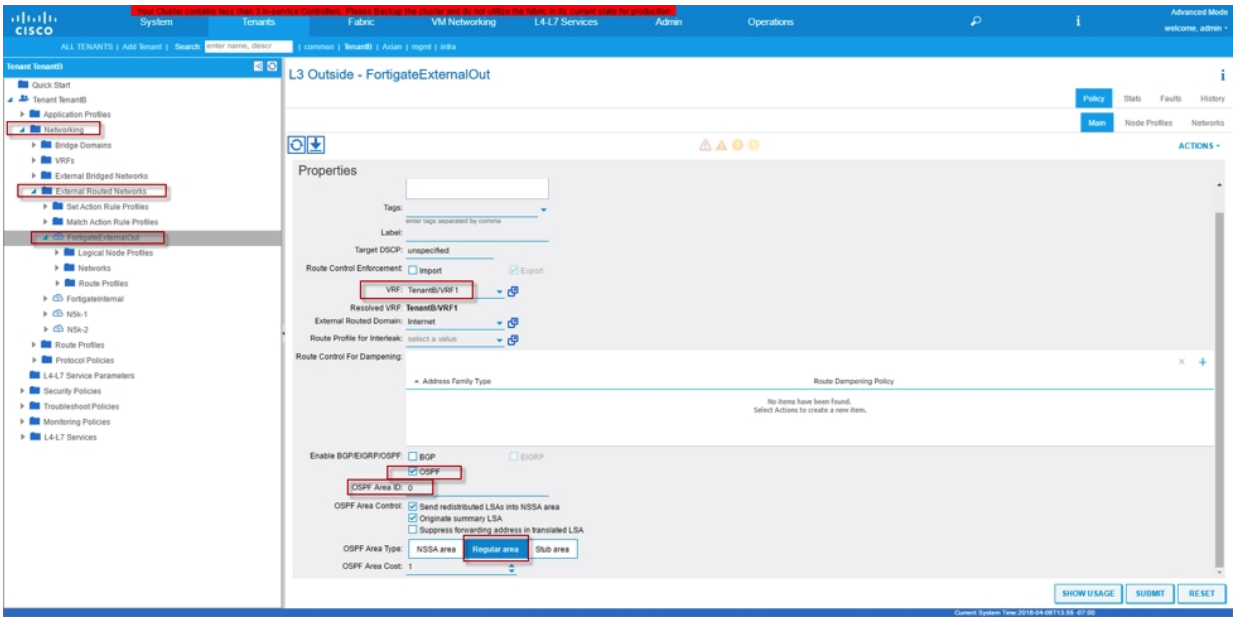


Configure Import/Export Route Control on Subnets for N5k-1 L3Out External EPG

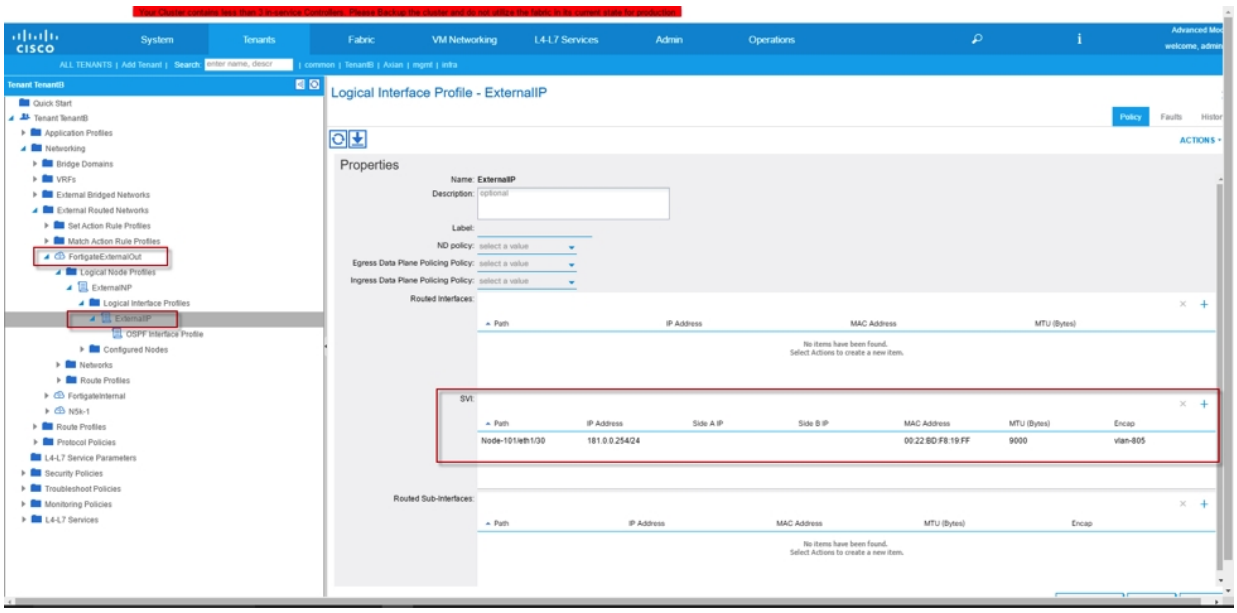


Configure L3Out for Fortigate External Interface (FortigateExternalOut) and associate with VRF1

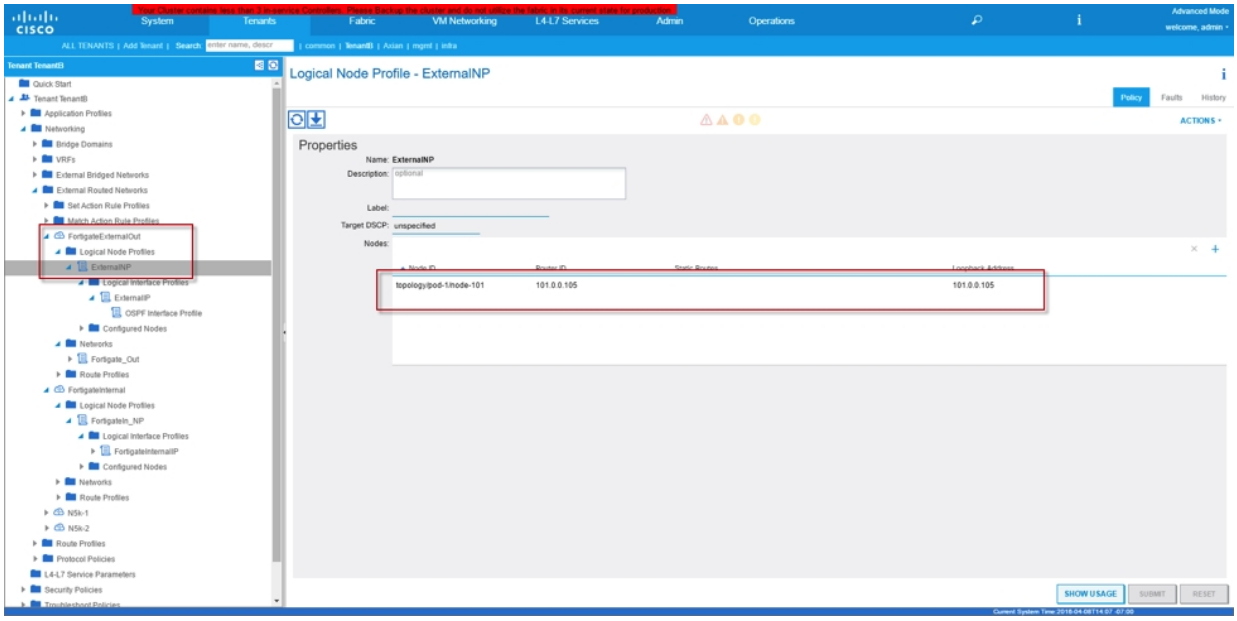
In our example, the route ID here must be the same as above (101.0.0.105), since both L3outs are on the same leaf switch.



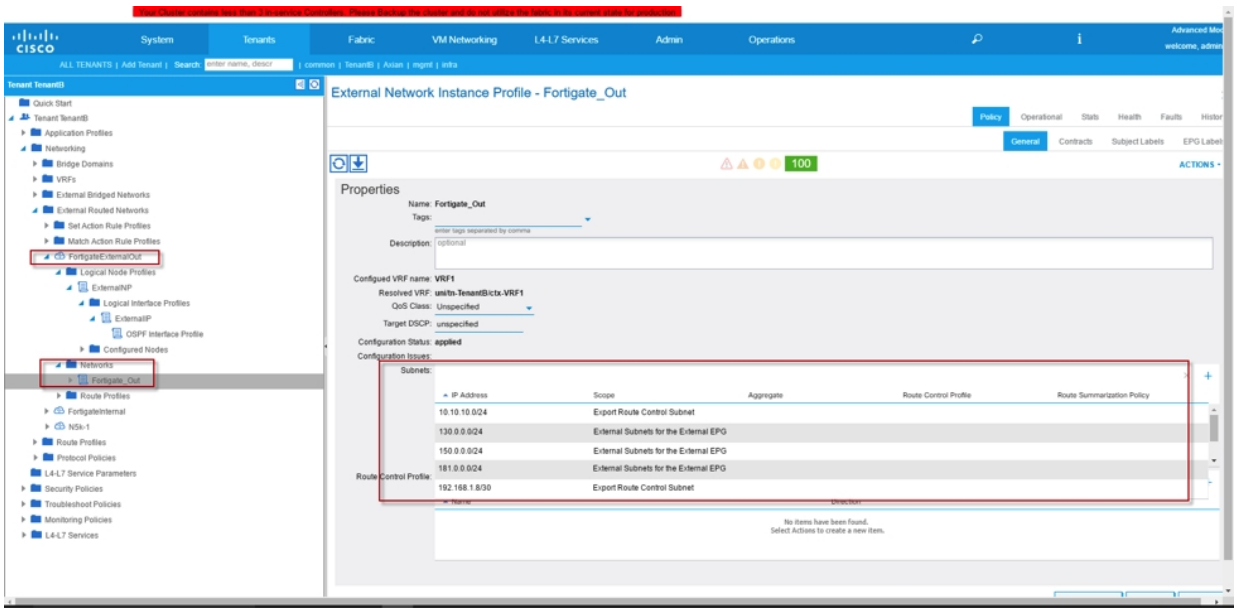
Configure SVI for L3Out Fortigate External out (FortigateExternalOut)



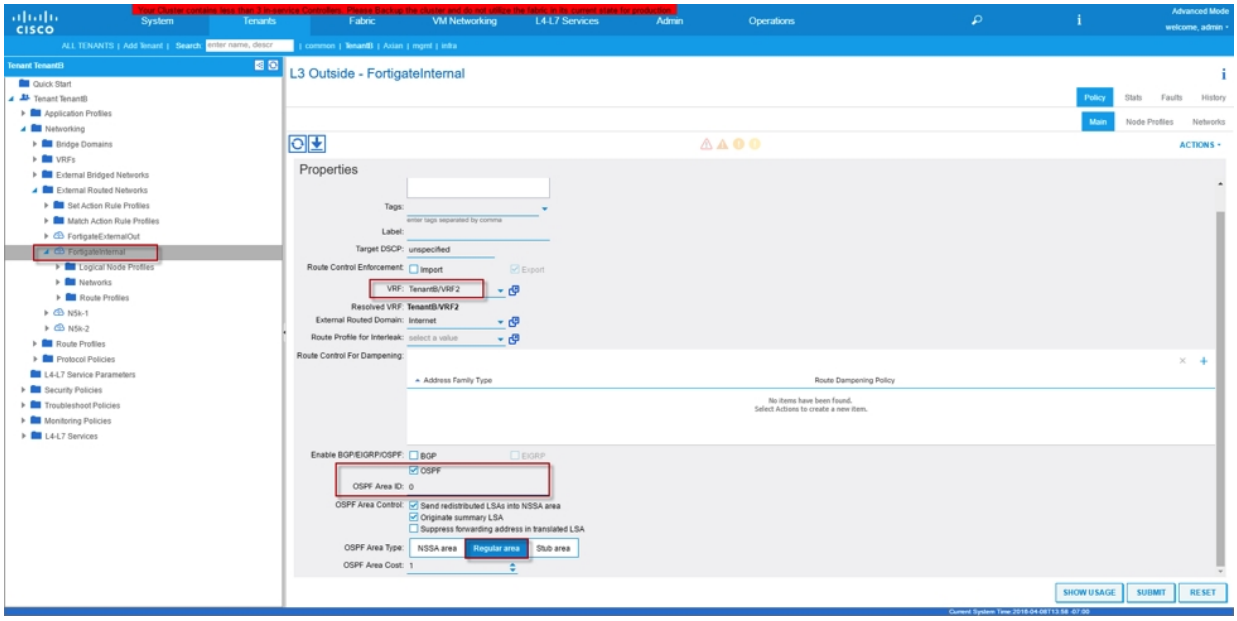
Configure Route ID for L3Out Fortigate External Out (FortigateExternalOut)



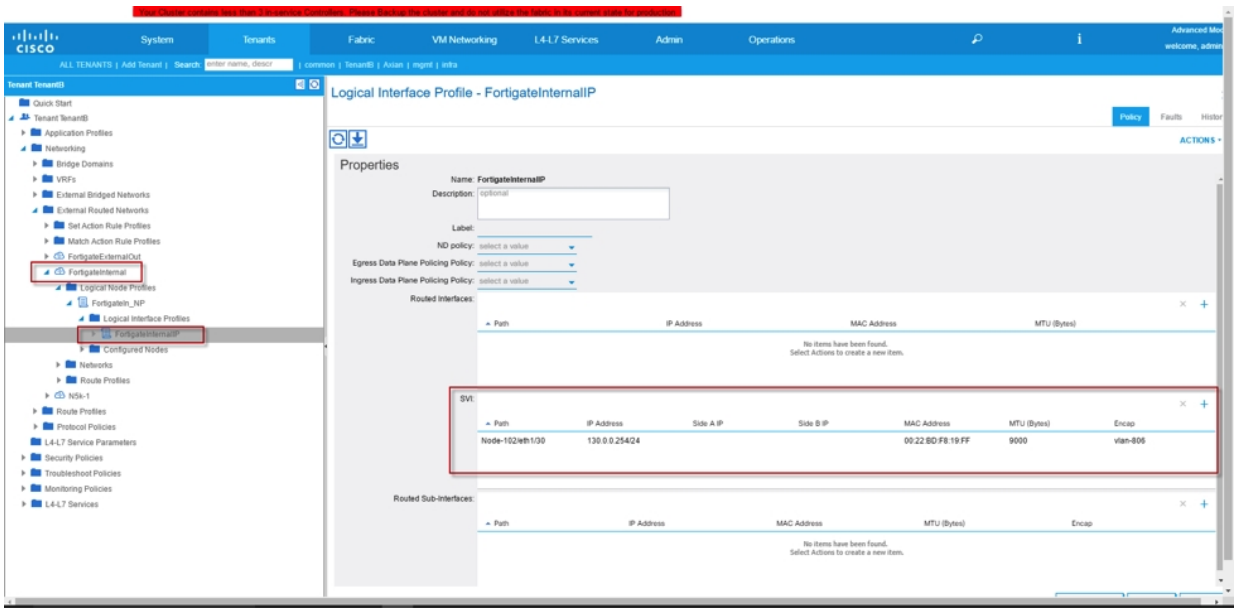
Configure Import/Export Route Control on Subnets for Fortigate External out



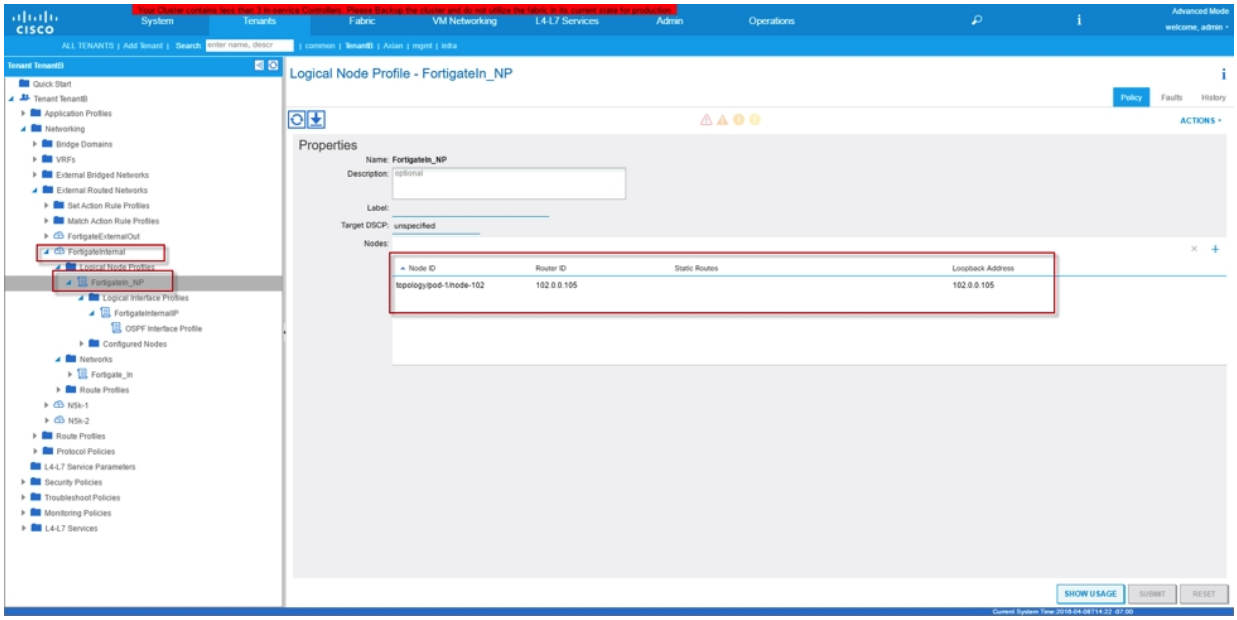
Configure L3Out for Fortigate Internal (FortigateInternal) and associate with VRF2



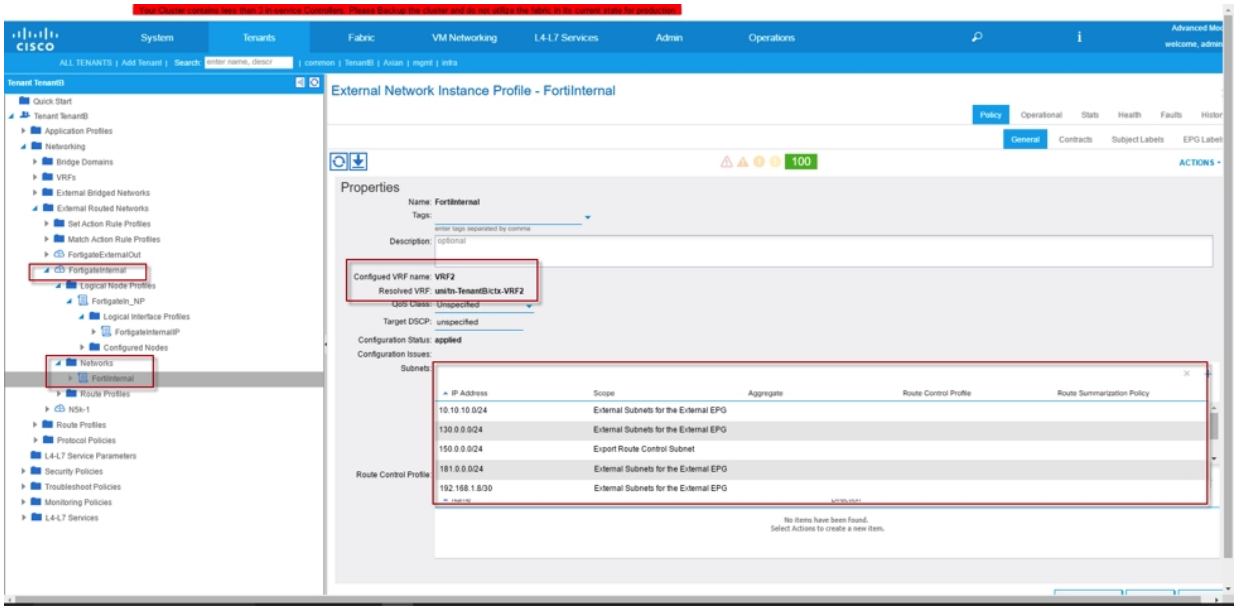
Configure SVI for L3Out Fortigate Internal (FortigateInternal)



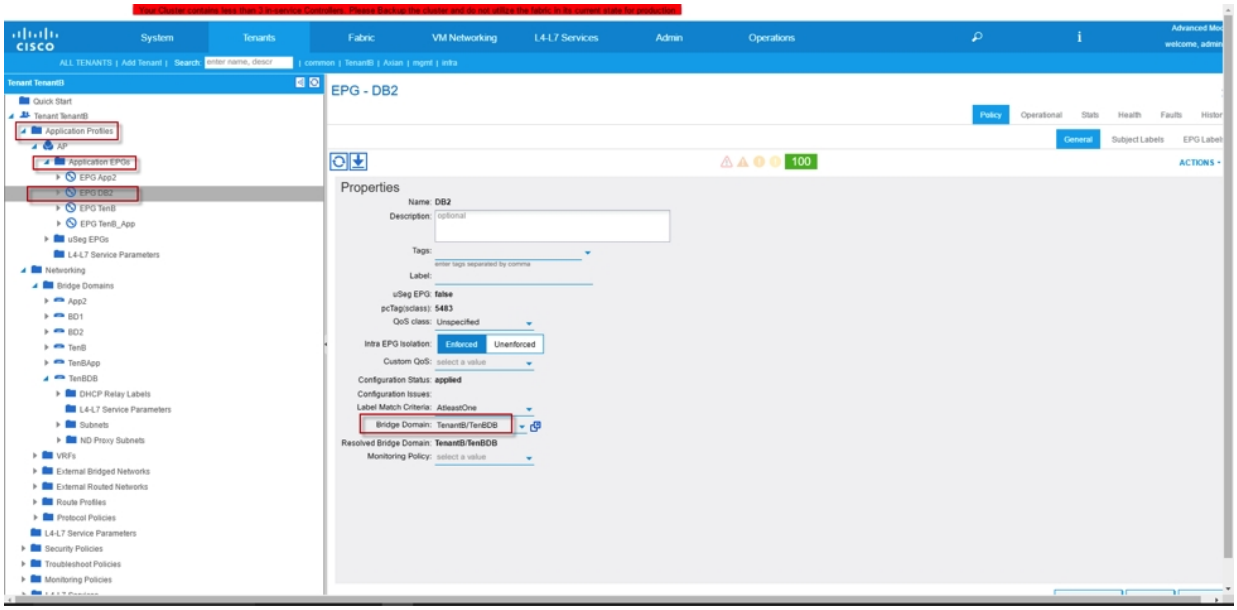
Configure Route ID for L3Out Fortigate Internal (FortigateInternal)

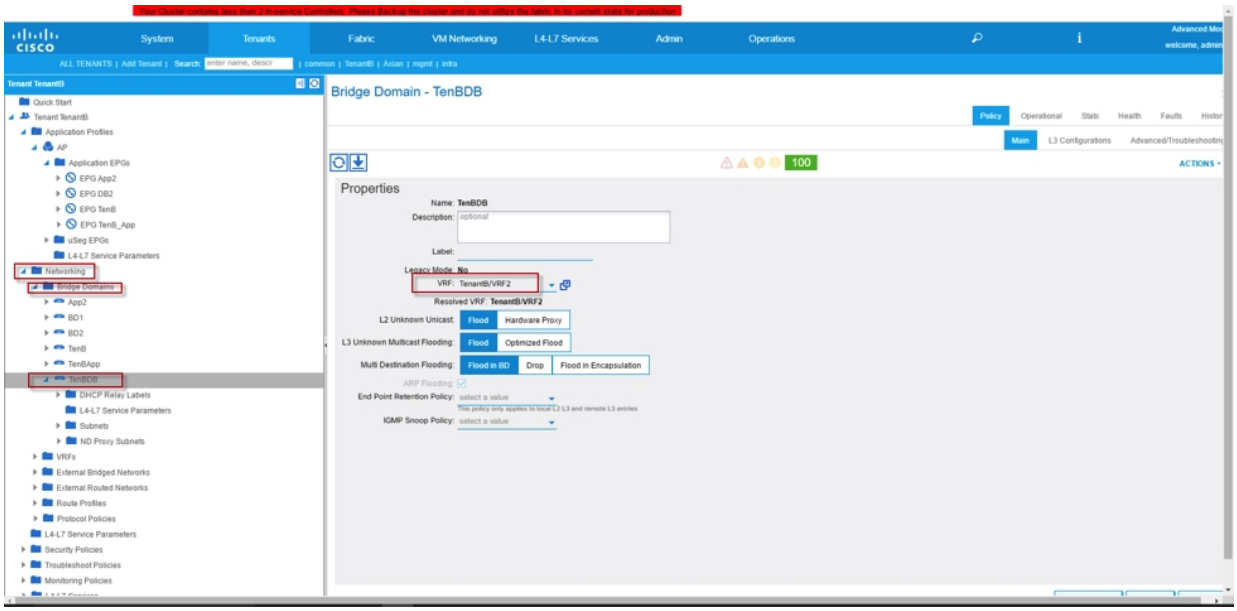


Configure Import/Export Route Control on Subnet for L3Out Fortigate Internal (FortigateInternal)

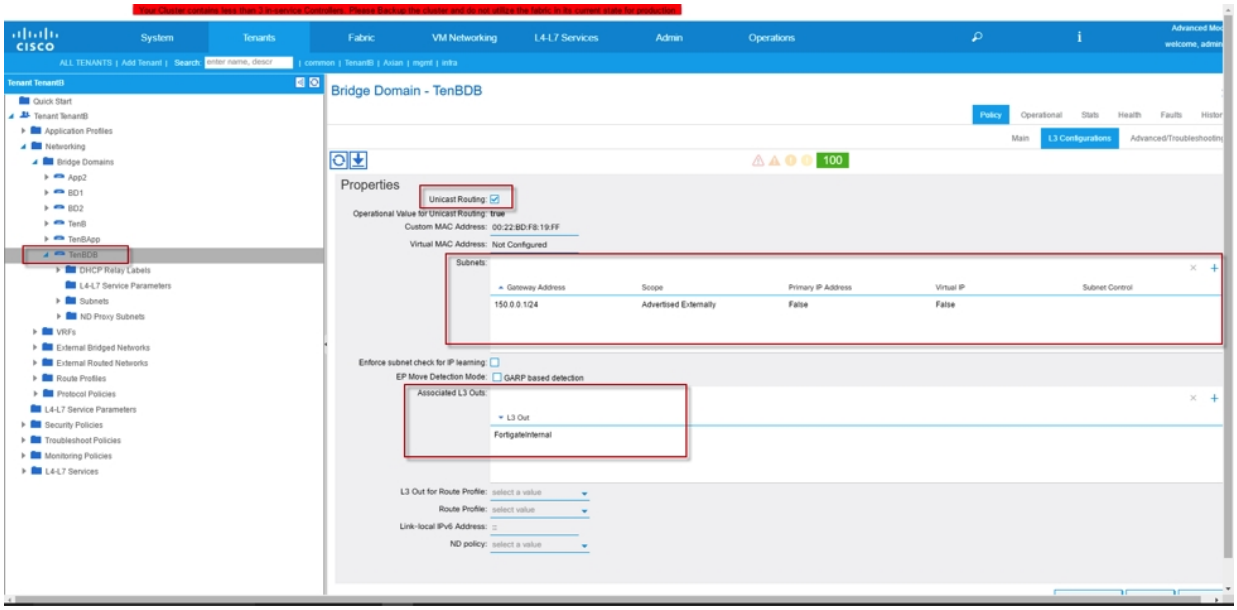


Associate EPG “DB2” to Bridge Domain “TenBDB” and attach Bridge Domain to VRF2

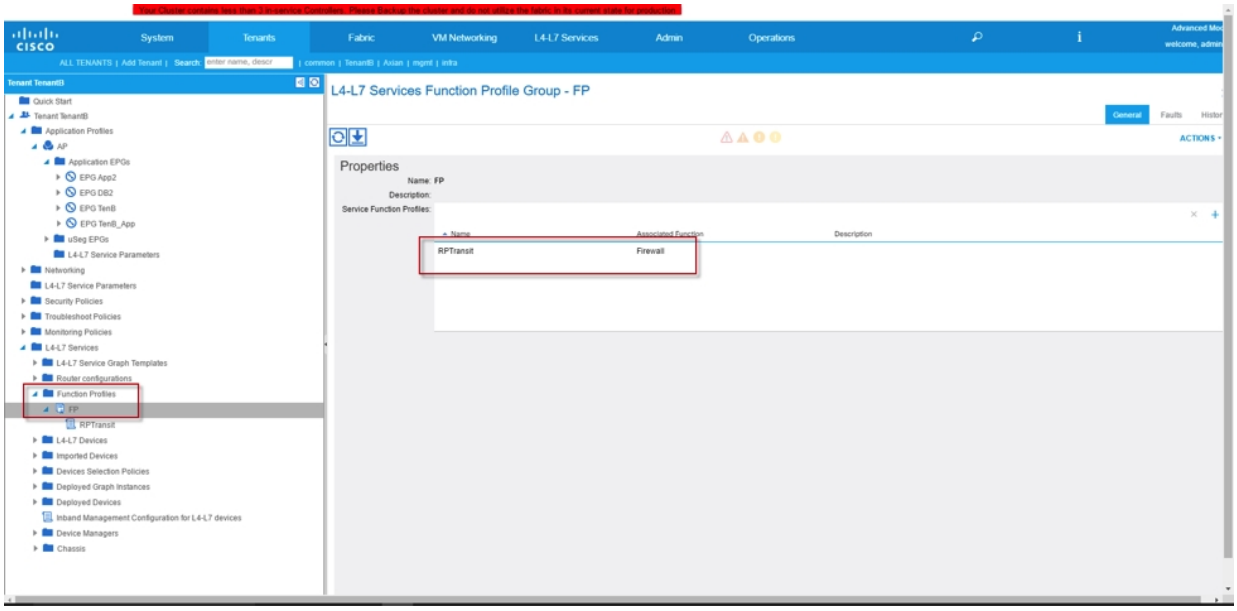


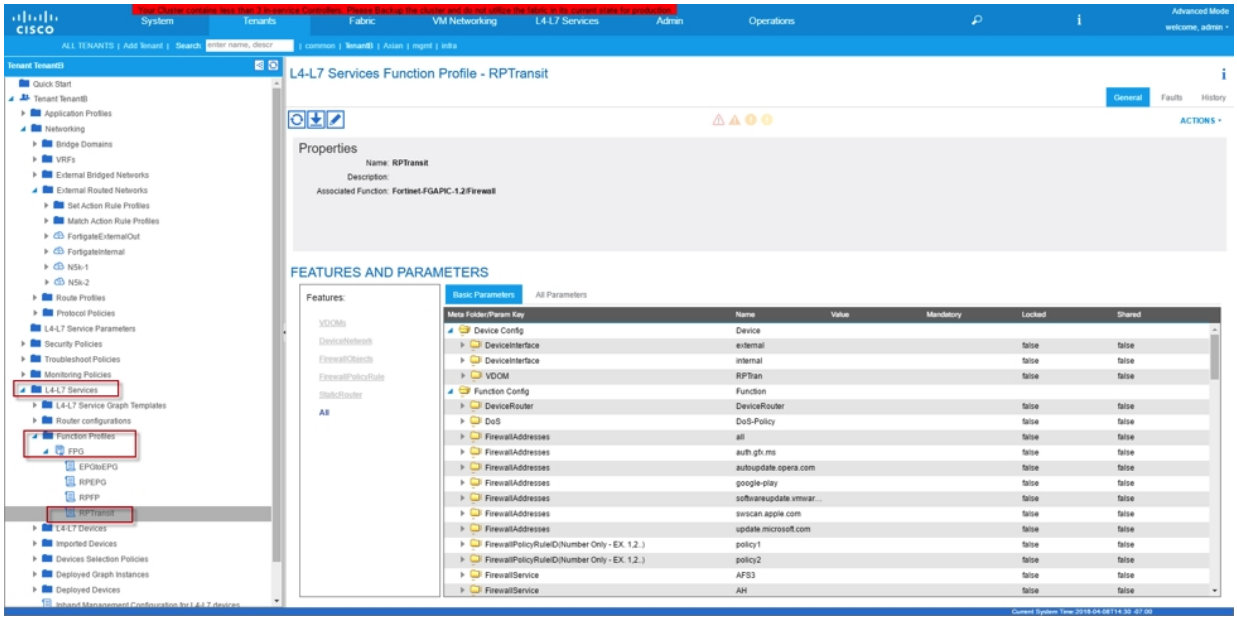


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Outs to “FortigateInternal”

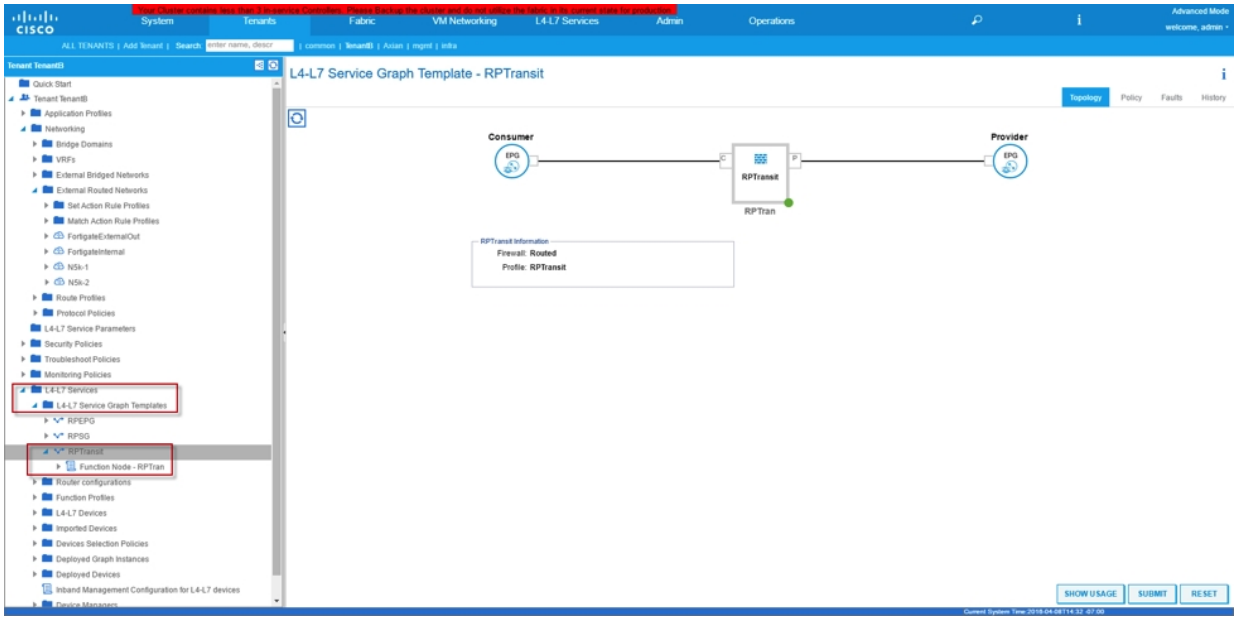


Create Functional Profile Group and Functional Profile from existing template

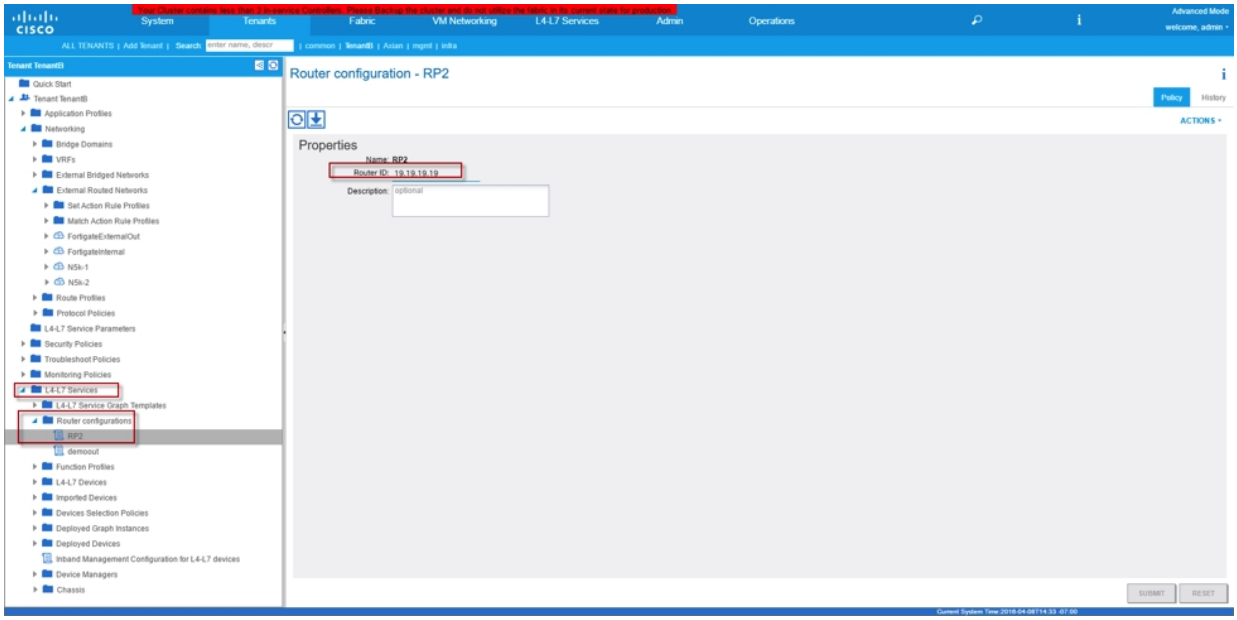




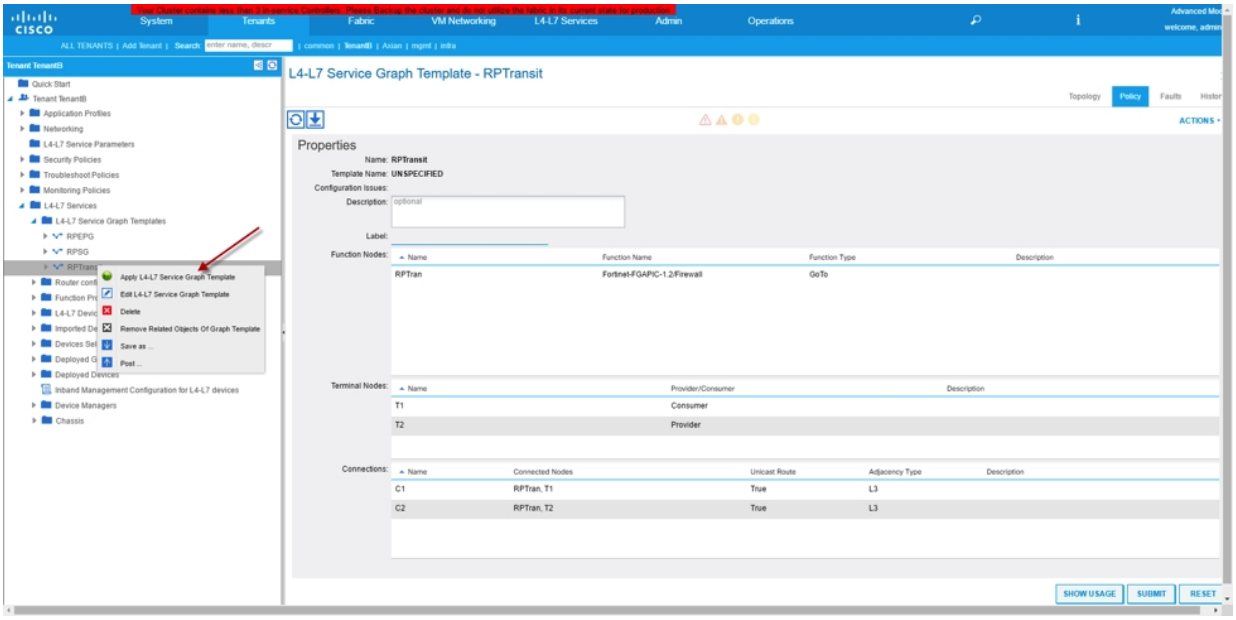
Create Service Graph template



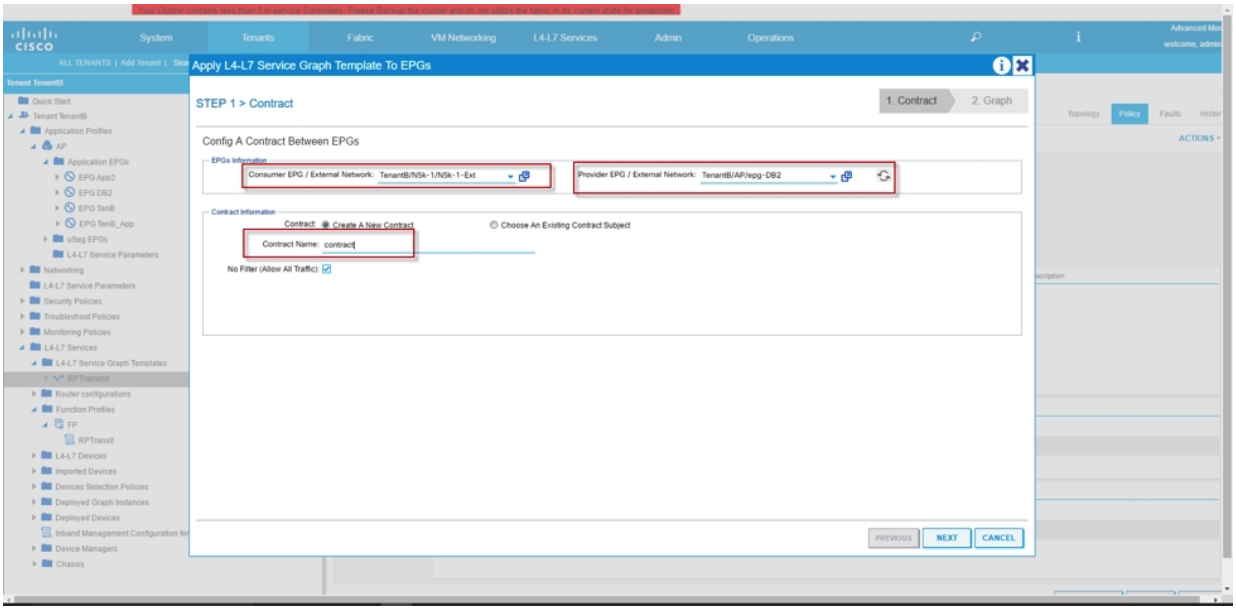
Create Router ID that will be used on the Service Appliance (Fortigate)



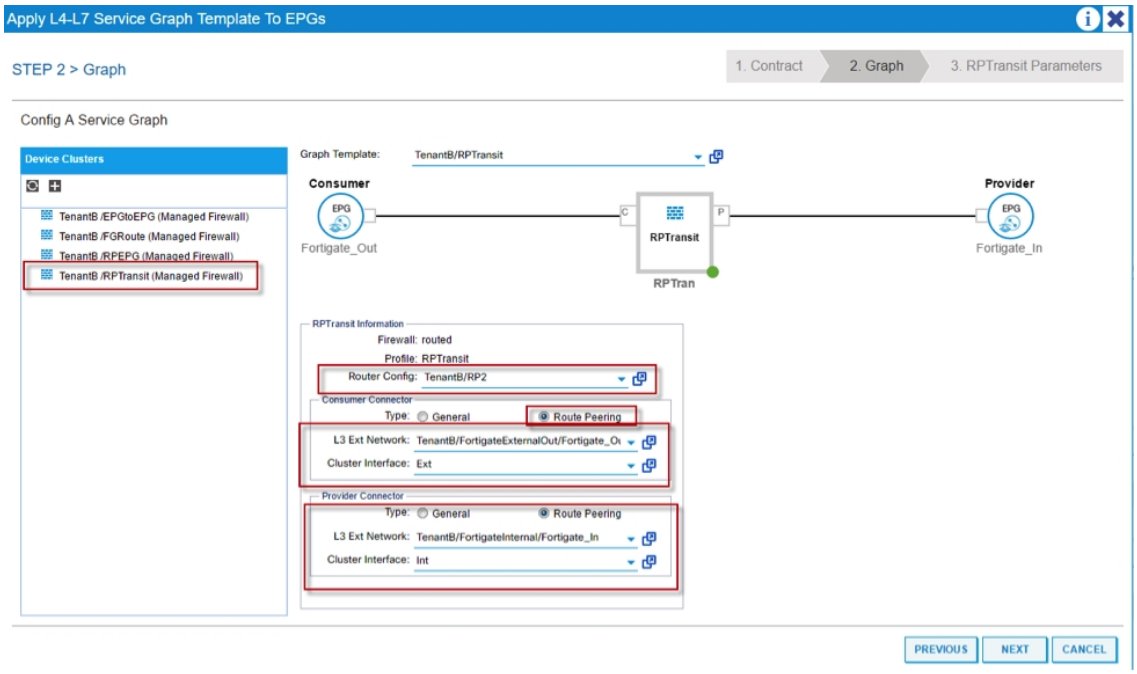
Deploy Service Graph



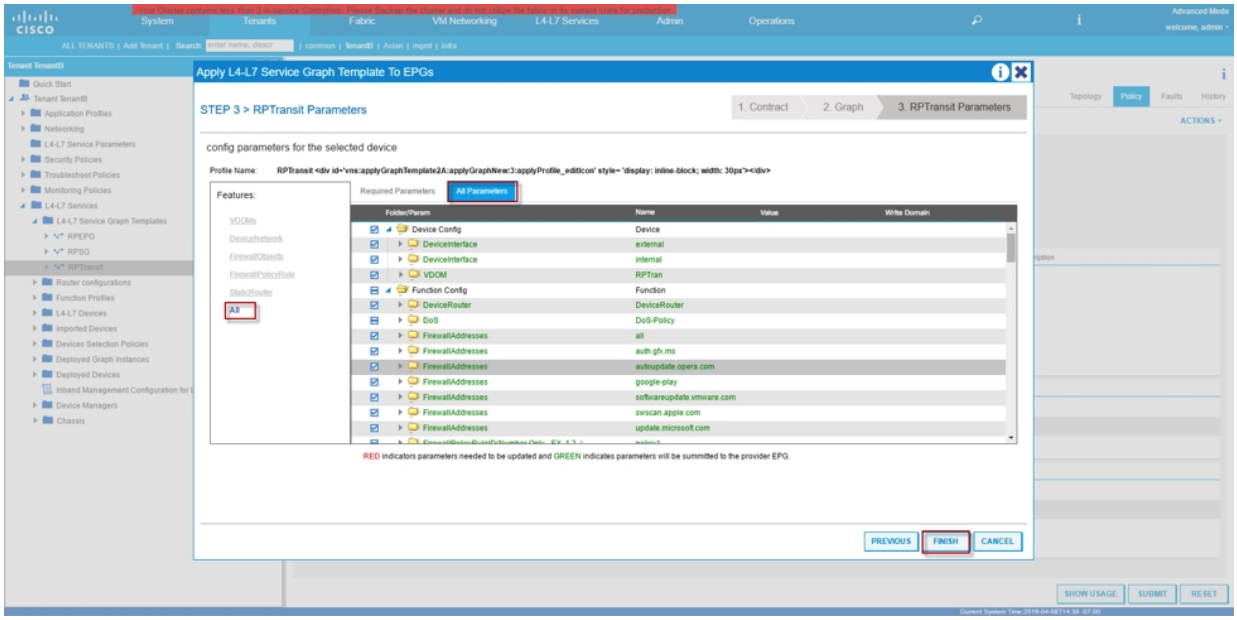
Consumer will be L3Outs facing external router. Provider is the internal EPG. In our case will be N5k-1 and DB2 respectively.



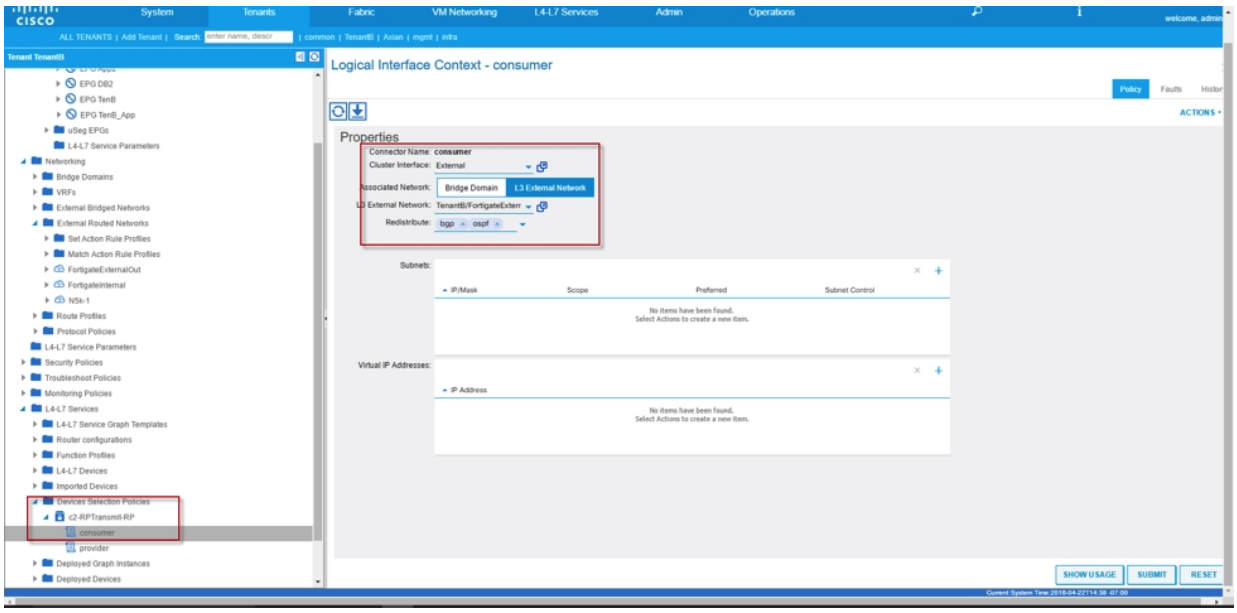
Route peering needs to be select for Internal and external connections. In our example, we used “FortigateExternalOut” and FortigateInternal” as External and Internal selections respectively.

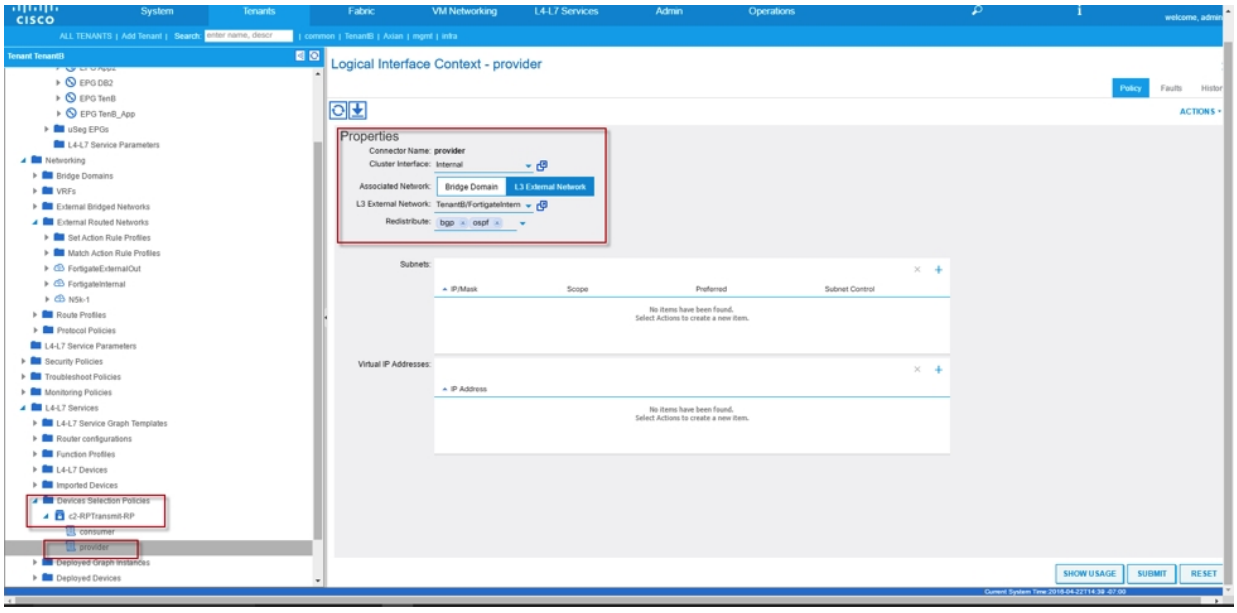


Last minute check to make sure configuration is good before hit “Finish” button

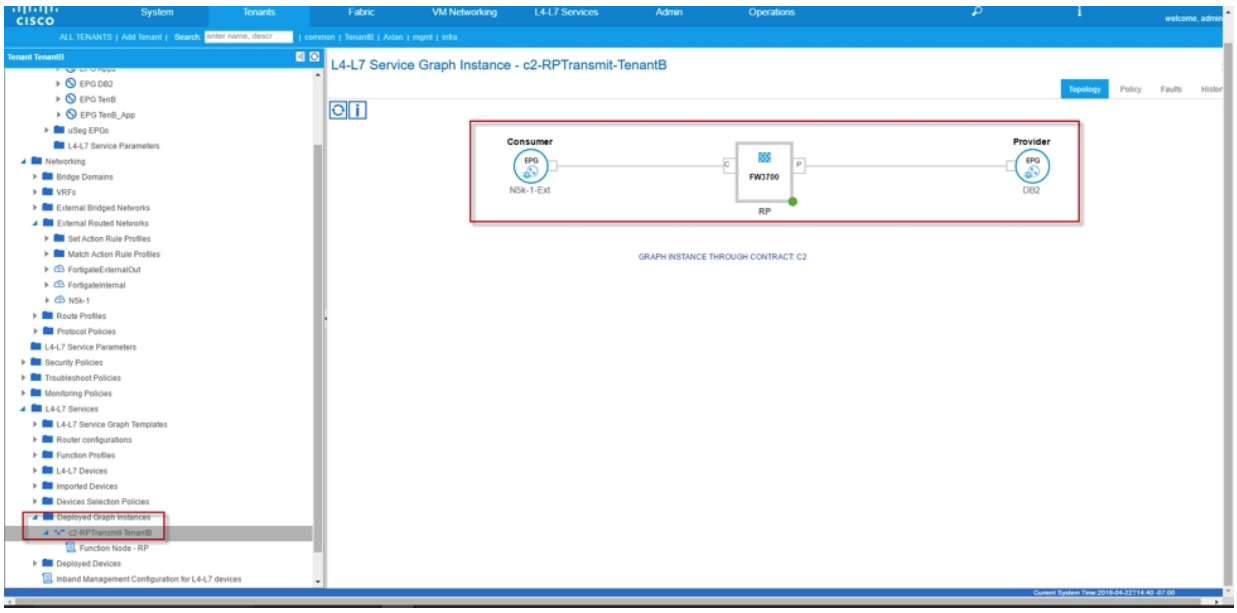


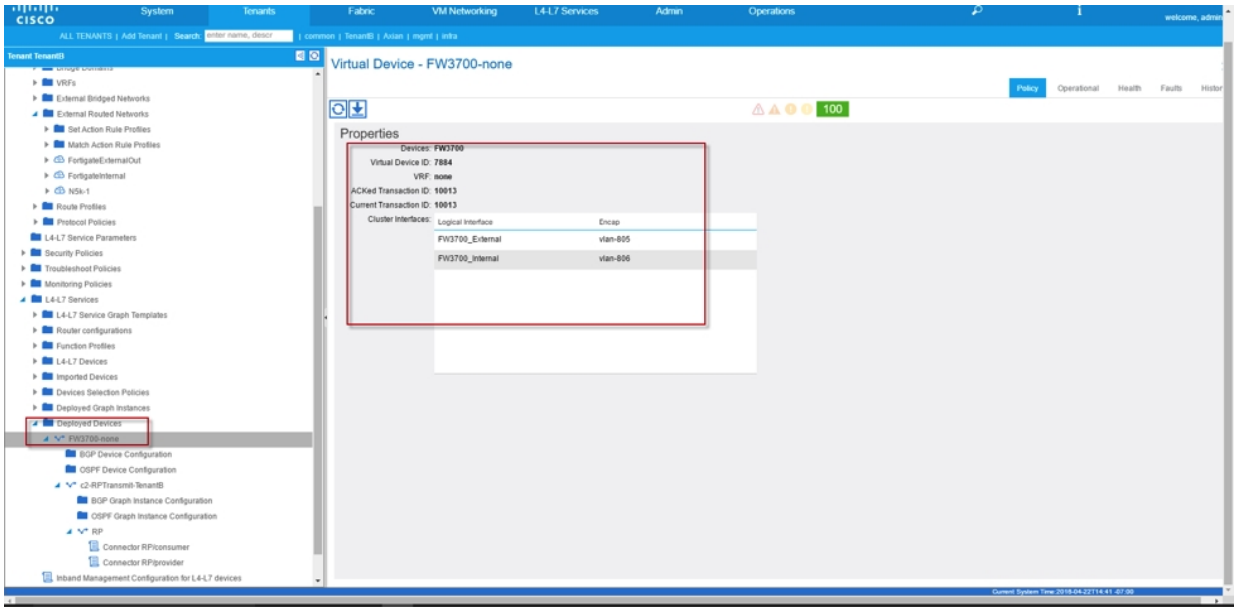
Check the status and verify Device Selection Policy





Verify deployed Graph Instance





Deploying High Availability Service with Cisco ACI and FortiGate

Pre-requisite

On Fortigate

- Configure Fortigate HA Pair (Active-Standby Mode). Please consult Fortinet support website for setting up HA procedures.

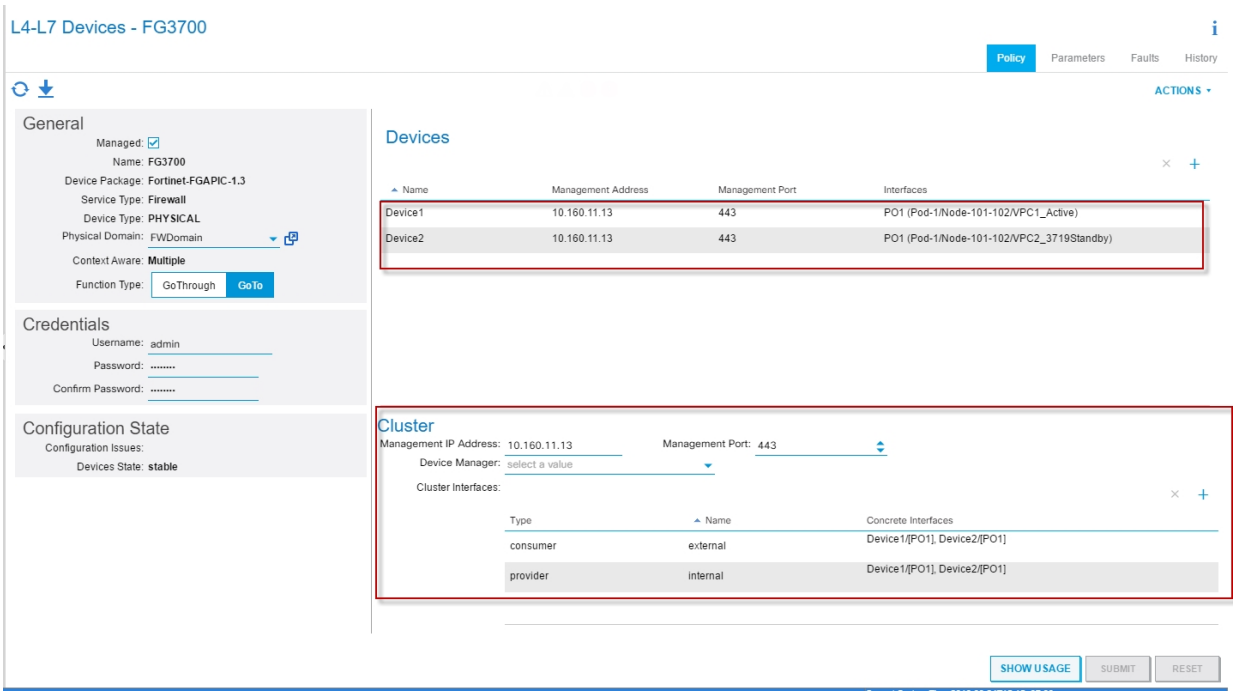
On APIC

- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- L4-L7 Device Package has imported into Cisco APIC

Work Flow

1. Create Go-Through Mode with HA enabled, then configure Device #1 and Device #2 on Cisco APIC
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

In general, the procedures to deploy a Go-Through mode HA scenario vs regular Go-Through mode deployment are identical with the exception of enabling HA during L4-L7 device configuration. User needs to select HA Cluster instead of Single Node for Mode selection; there will be two devices appear on the screen where user will input the same Active Fortigate IP address and the corresponding connection ports between Fortigates and Cisco APIC for both devices. Please see below screen shot for reference.


L4-L7 Devices - FG3700
Policy
Parameters
Faults
History
ACTIONS
General
Managed:
Name: FG3700
Device Package: Fortinet-FGAPIC-1.3
Service Type: Firewall
Device Type: PHYSICAL
Physical Domain: FWDomain
Context Aware: Multiple
Function Type: GoThrough GoTo
Credentials
Username: admin
Password:
Confirm Password:
Configuration State
Configuration Issues:
Devices State: stable
Devices
Name
Management Address
Management Port
Interfaces
Device1
10.160.11.13
443
PO1 (Pod-1/Node-101-102/VPC1_Active)
Device2
10.160.11.13
443
PO1 (Pod-1/Node-101-102/VPC2_3719Standby)
Cluster
Management IP Address: 10.160.11.13
Management Port: 443
Device Manager: select a value
Cluster Interfaces:
Type
Name
Concrete Interfaces
consumer
external
Device1/[PO1], Device2/[PO1]
provider
internal
Device1/[PO1], Device2/[PO1]
SHOW USAGE
SUBMIT
RESET

Deploying Firewall service with Fortigate-VM and VMware

Pre-requisite

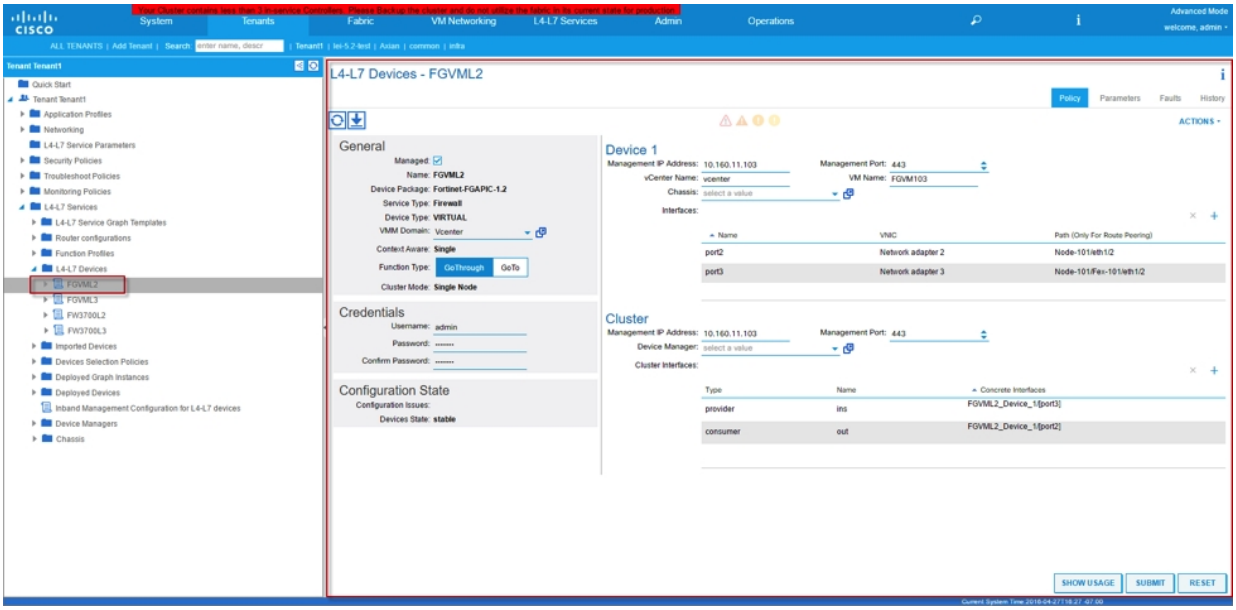
- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer4-7 Device Package has imported into Cisco APIC

Work Flow

1. Create Go-Through mode Fortigate VM Devices on Cisco APIC
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

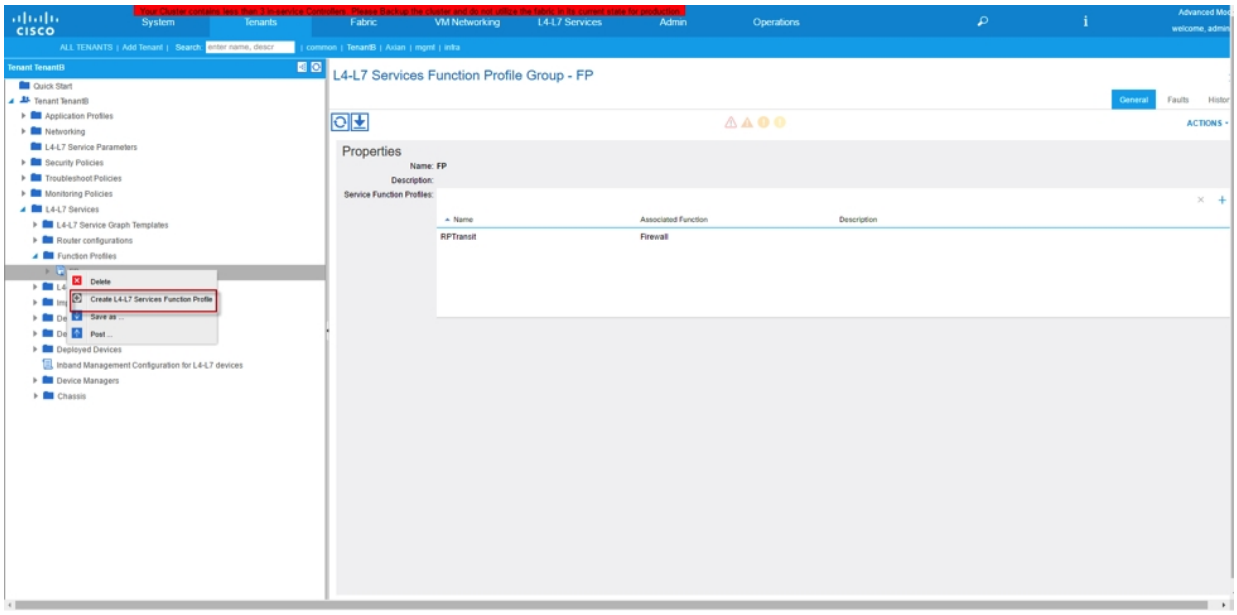
Configuration

Create Layer 4-L7 Device on Cisco APIC



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation

Device Config

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM.

Similar to above notes, for Go-To Mode, please modify the IP address field otherwise leave the default for Go-Through Mode.

Function Config

Function Config consist of:

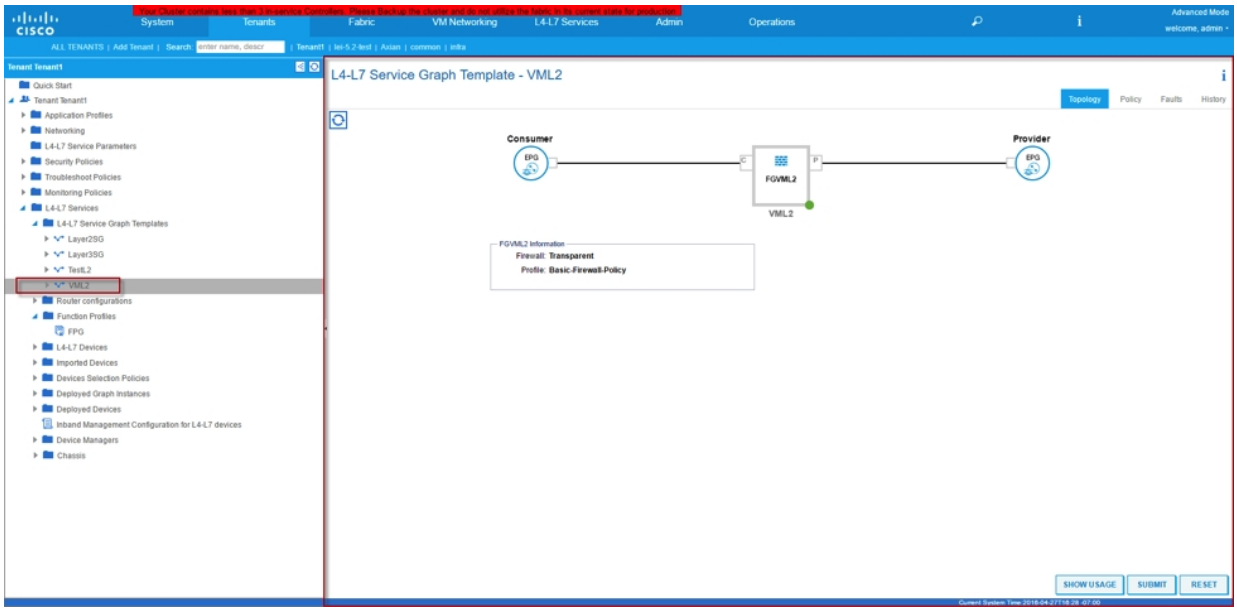
- **Network**
  - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
  - This folder is the container for following list of Folders:
    a. FWServiceFolder – Firewall Service Object container
    b. IPv4/IPv6 DoS Policy – Dos Policy configuration
    c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
    d. IPv4 Policy – Firewall Policy Rule container

e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
f. ScheduleFolder – Schedule container

- **VDOM-Folder**
  - VDOM internal and external interfaces

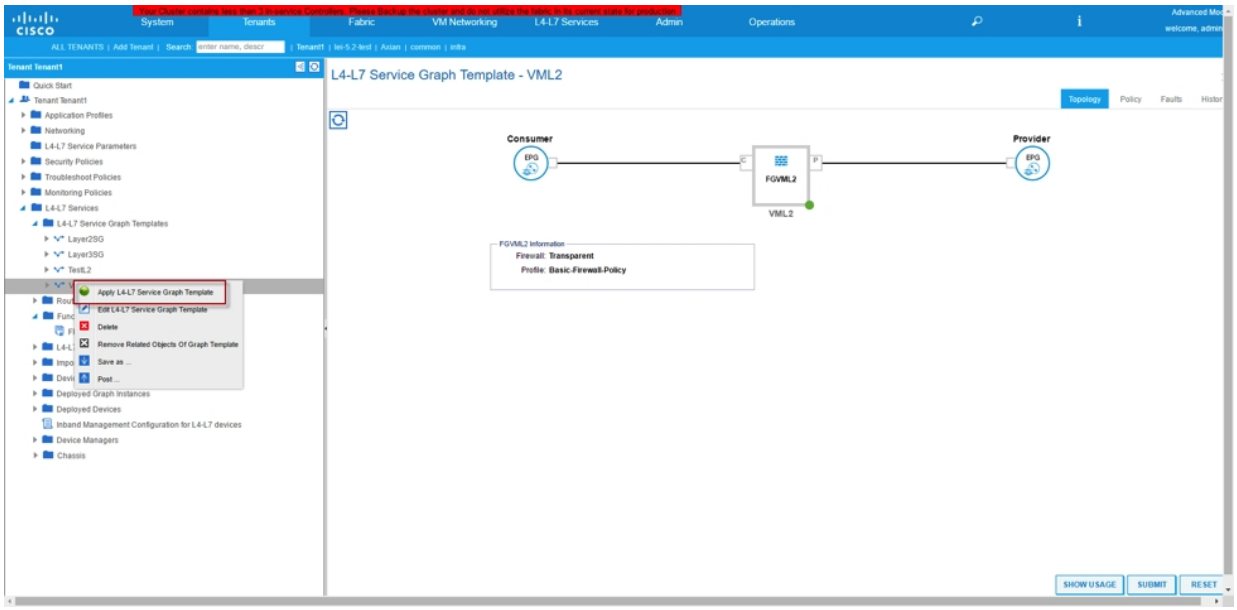
Create Service Graph

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

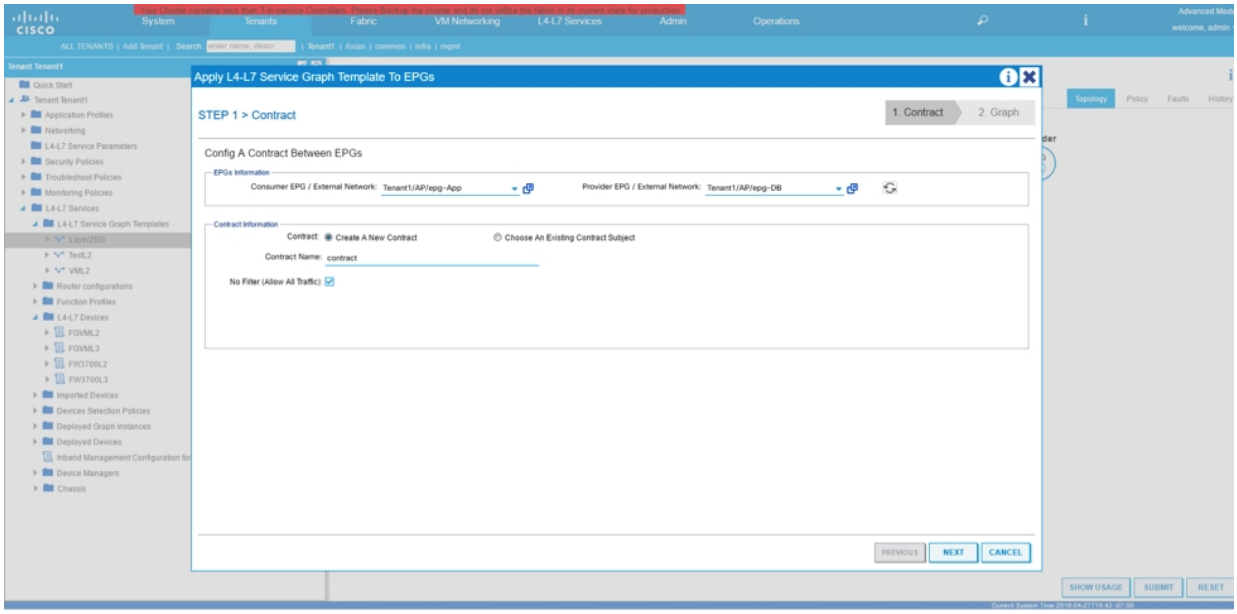


Deploy Service Graph

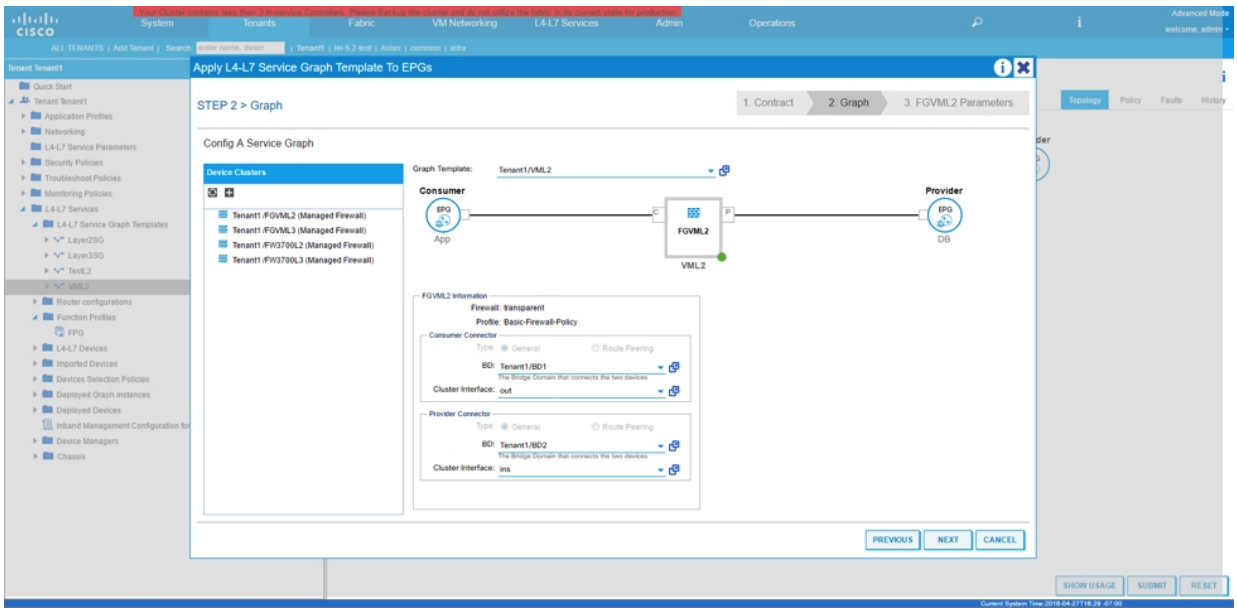
Once we combined the Firewall configuration and associated device together, we are ready to deploy the service Graph to create a VDOM.



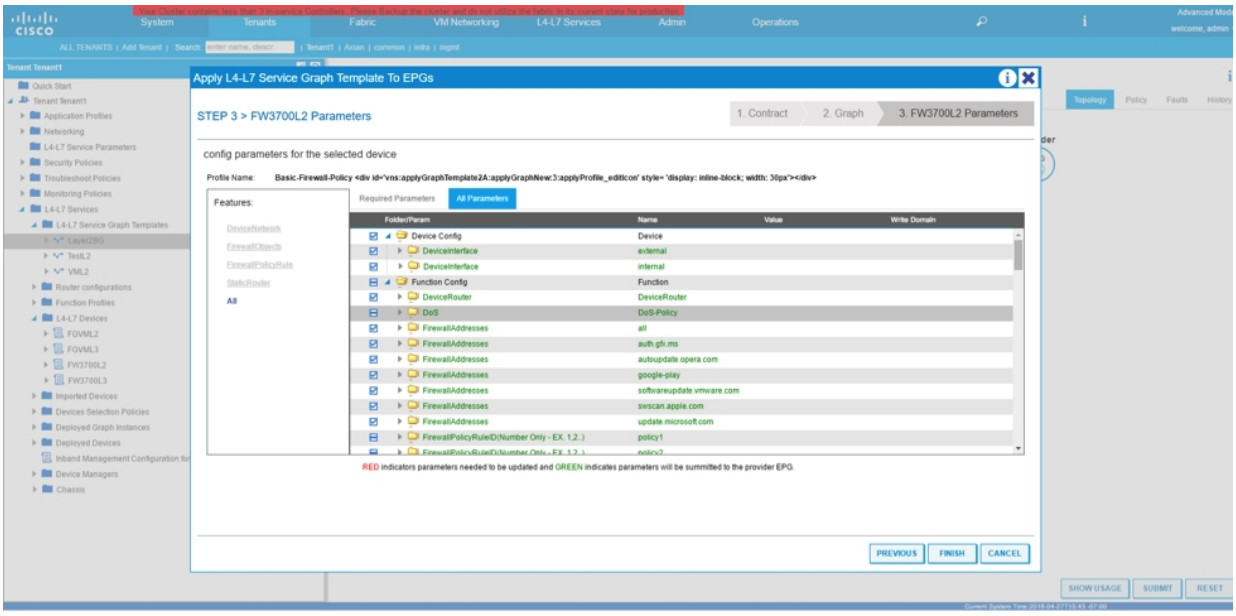
On next screen select the Consumer and provider EPGs and assign a contract name or select a pre-define contract.



Next screen select the logical interfaces defined during the creation of Layer4-7 Device.



Next screen to the last minute check to ensure everything is accordingly before deploy. If ok, then hit the submit button.


Apply L4-L7 Service Graph Template To EPGs
STEP 3 > FW3700L2 Parameters
1. Contract
2. Graph
3. FW3700L2 Parameters
config parameters for the selected device
Profile Name:
Basic-Firewall-Policy
Features:
Required Parameters
All Parameters
Folder/Param
Name
Value
Write Domain
Device Config
Device
DeviceInterface
external
DeviceInterface
internal
Function Config
Function
DeviceRouter
DeviceRouter
DoS
DoS-Policy
FirewallAddresses
all
FirewallAddresses
auth.gfx.ms
FirewallAddresses
autoupdate.opera.com
FirewallAddresses
google-play
FirewallAddresses
softwareupdate.vmware.com
FirewallAddresses
swscan.apple.com
FirewallAddresses
update.microsoft.com
FirewallPolicyRuleID(Number Only - EX. 1,2..)
policy1
RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.
PREVIOUS
FINISH
CANCEL
SHOW USAGE
SUBMIT
RESET

Deploy the firewall device shared by multiple service graphs

Pre-requisite

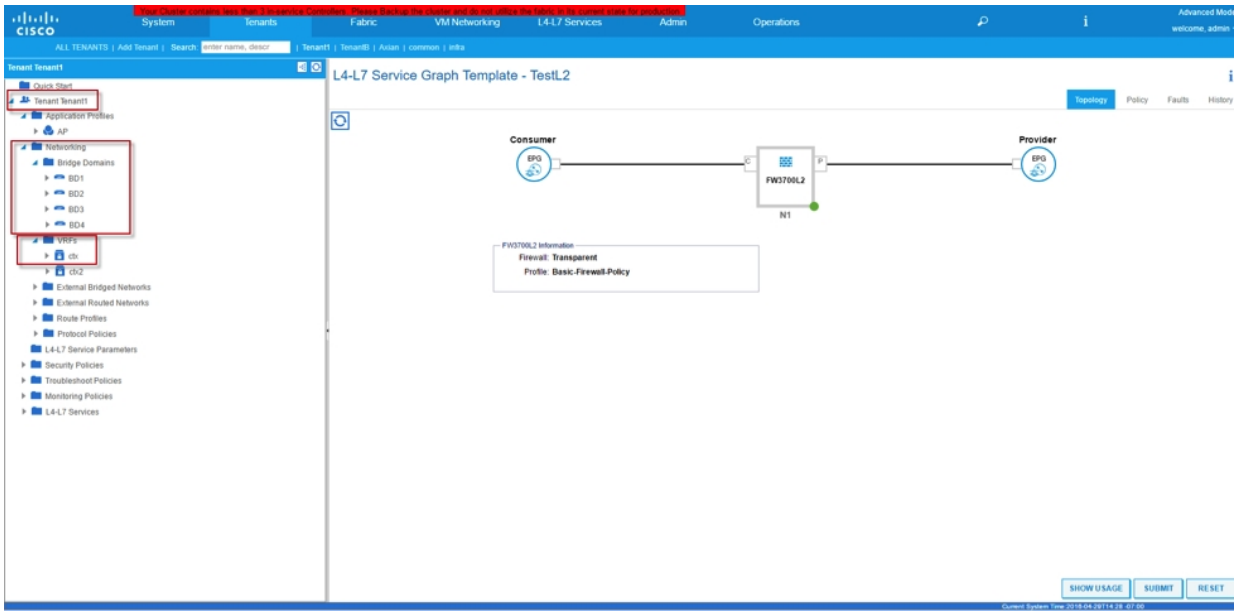
- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- Layer4-7 Device Package has imported into Cisco APIC

Work Flow:

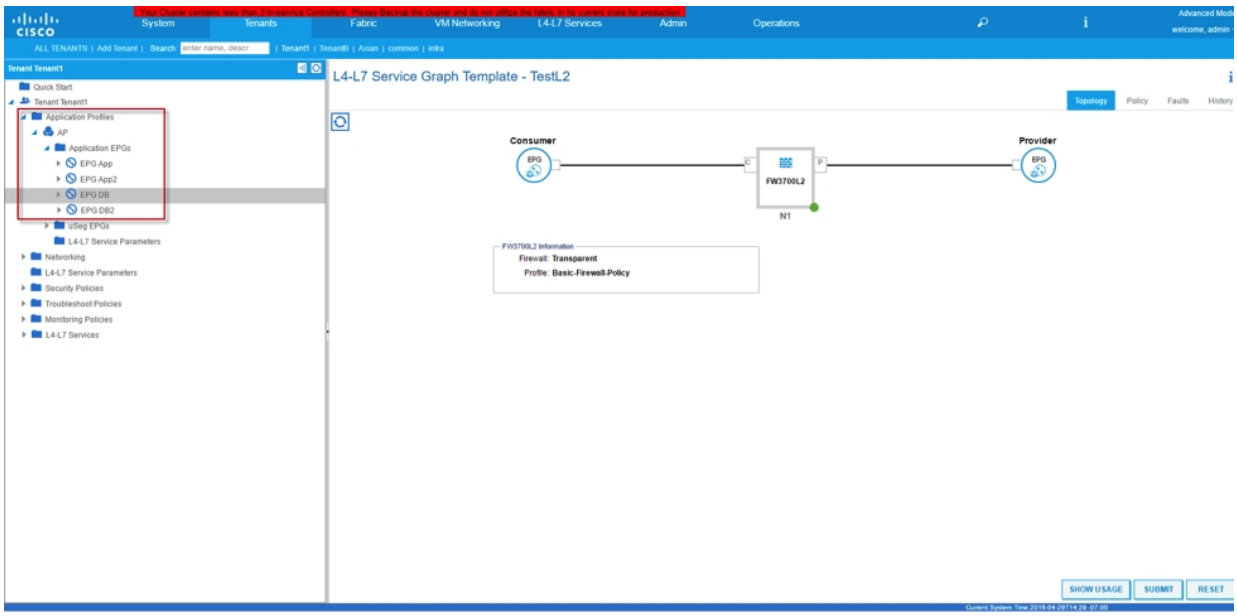
1. Create Tenant (“Tenant1” in our example)
2. Create VRF (“ctx” in our example)
3. Create 4 Bridge Domains (“BD1”, “BD2”, “BD3” and “BD4” in our example)
4. Associate Bridge Domains to VRF
5. Create 4 EPGs (“App” , “App2”, “DB”, “DB2” in our example)
6. Associate EPGs to Bridge Domains (EPG “App”, “App2”, “DB” and “DB2” are mapped to Bridge Domain “BD1”, “BD2”, “BD3” and “BD4” respectively in our example)
7. Create Go-Through mode Device on Cisco APIC and define 4 logical interfaces
8. Create Functional Profile
9. Create 2 Service Graph Templates
10. Deploy Service Graph 2 times on the same device but with different EPG pairs

Configuration

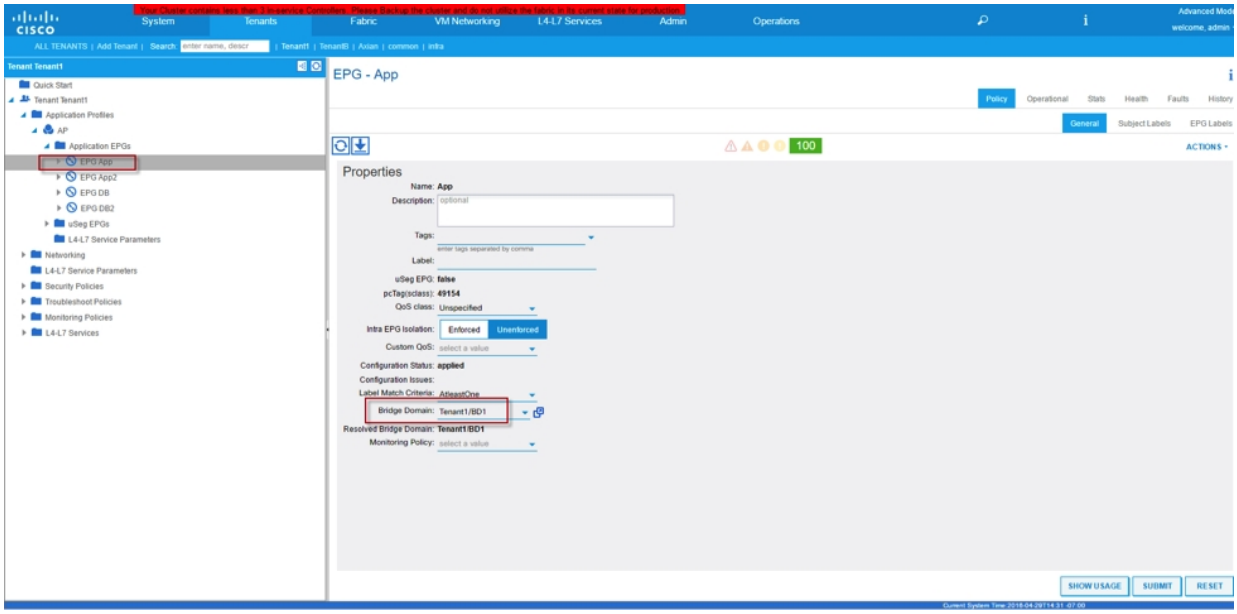
Create Tenant, VRF and 4 Bridge Domains on Cisco APIC

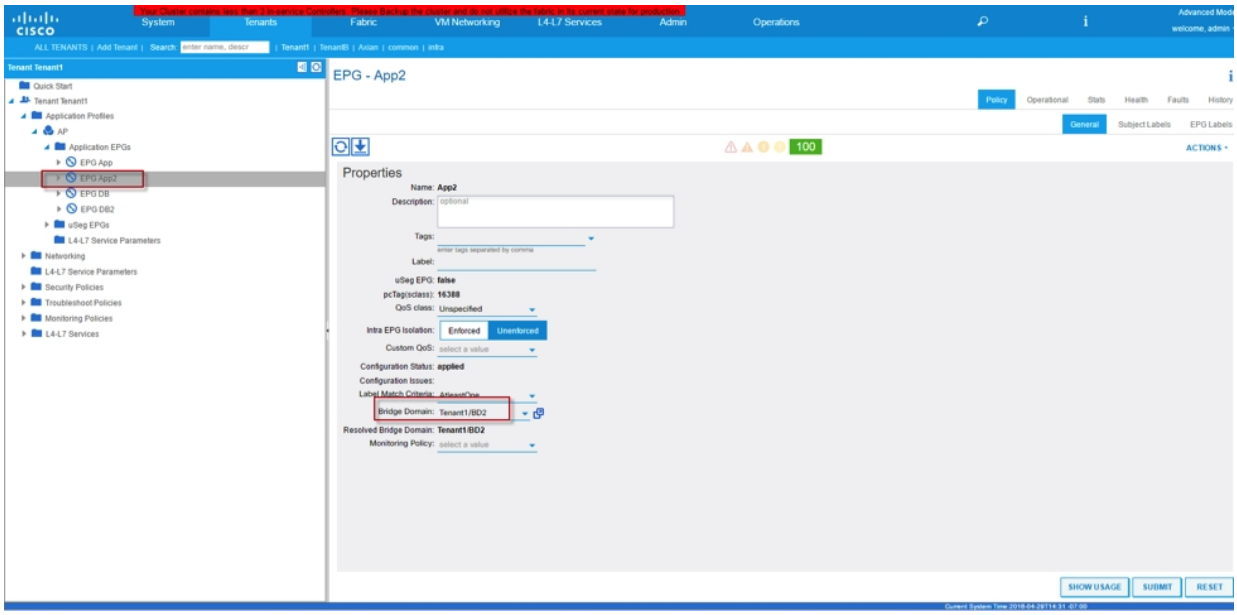


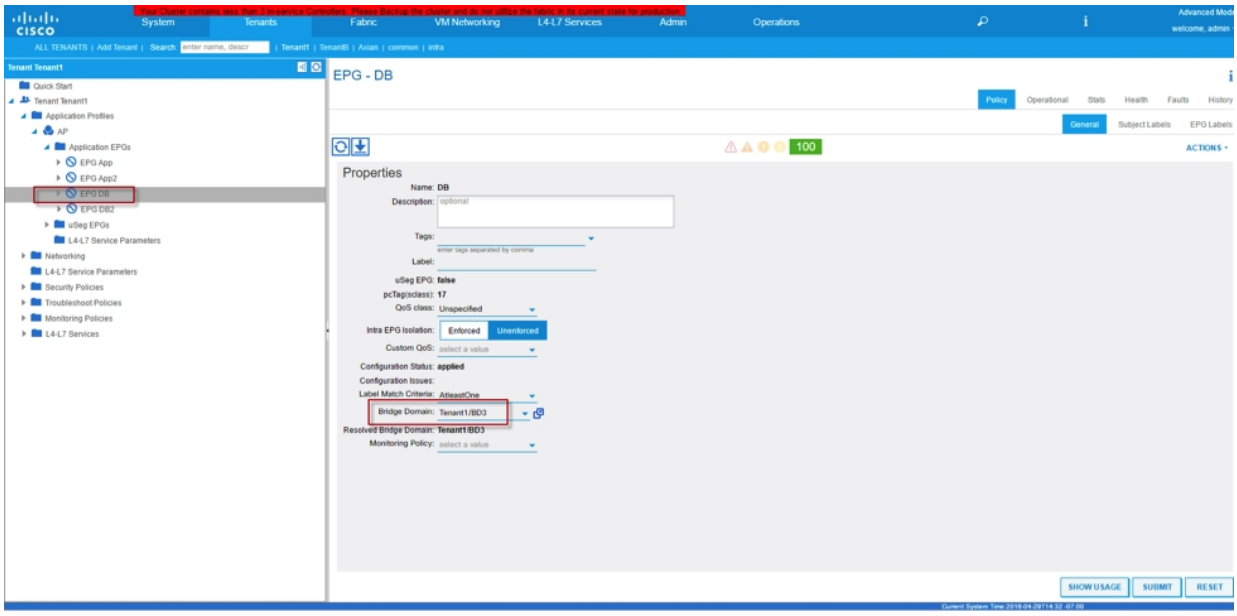
Create 4 EPGs

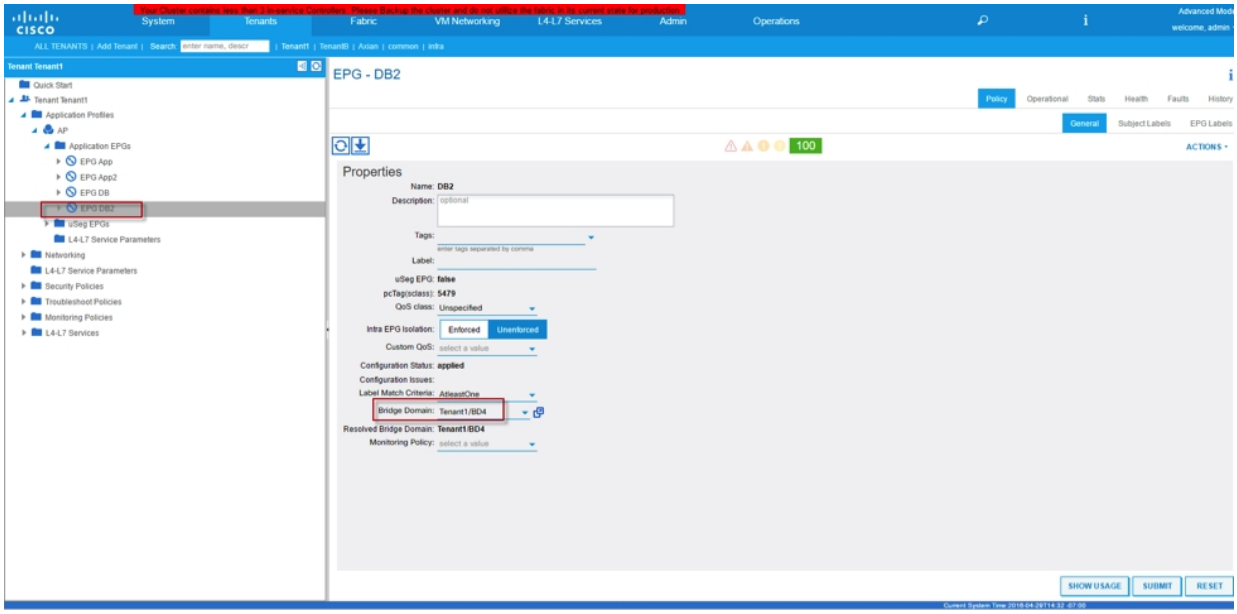


Associate EPG “App”, “App2”, “DB” and “DB2” to Bridge Domain “BD1”, “BD2”, “BD3” and “BD4” respectively

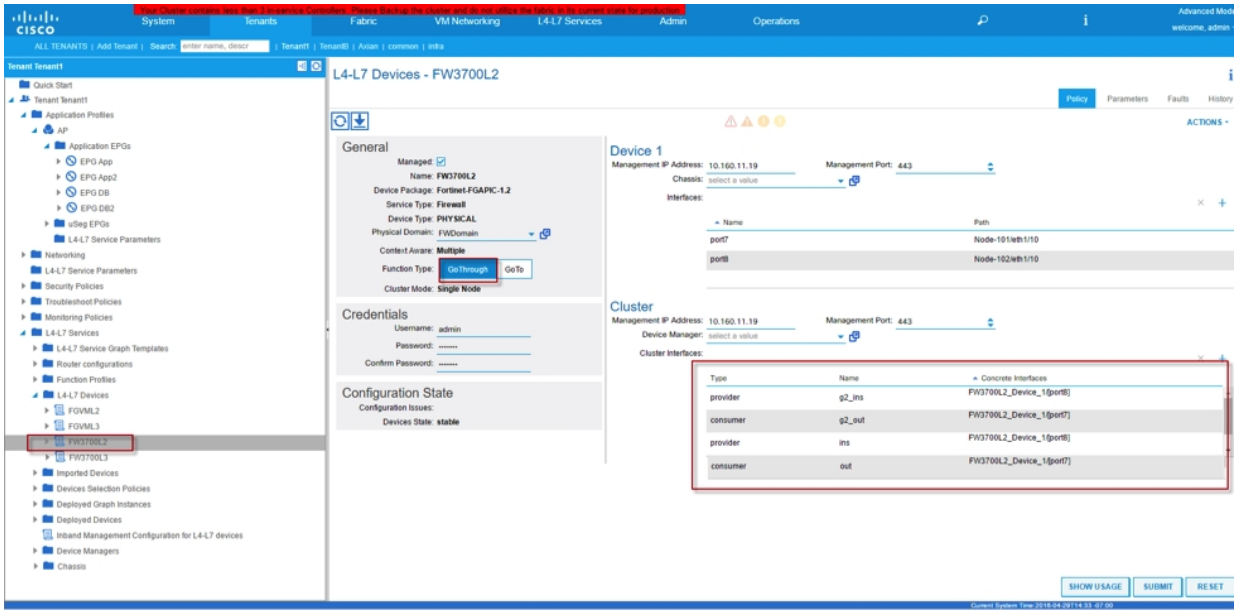





EPG - DB
Properties
Name: DB
Description: optional
Tags:
Label:
uSeg EPG: false
pcTag(sclass): 17
QoS class: Unspecified
Intra EPG Isolation: Enforced Unenforced
Custom QoS: select a value
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: Tenant1/BD3
Resolved Bridge Domain: Tenant1/BD3
Monitoring Policy: select a value
SHOW USAGE
SUBMIT
RESET

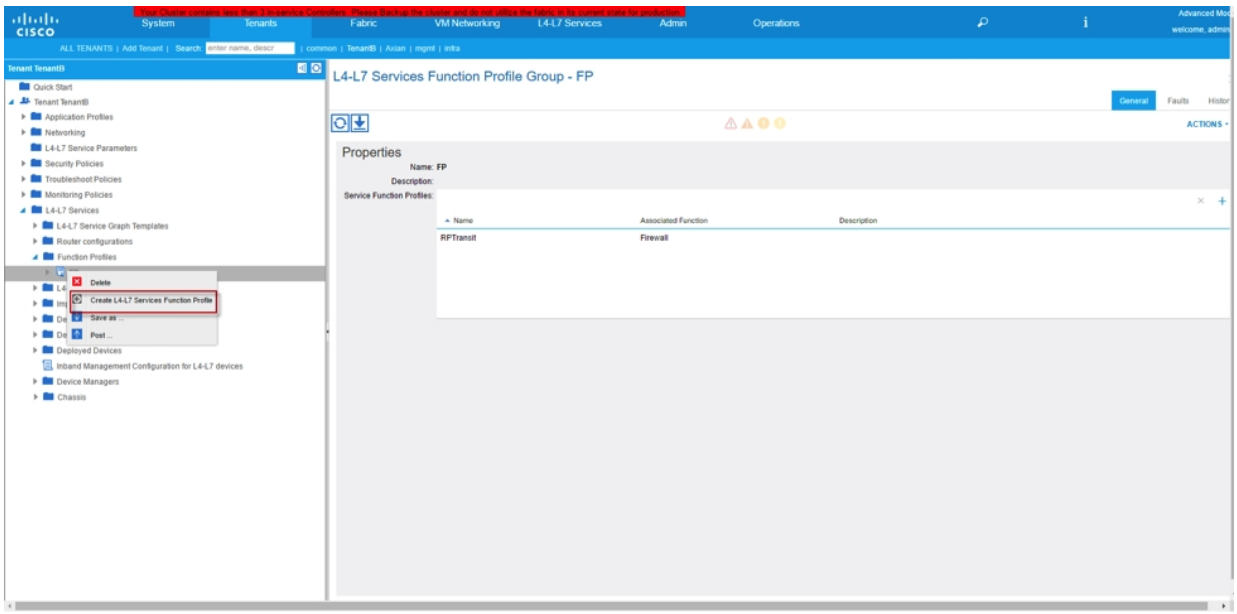

EPG - DB2
Properties
Name: DB2
Description: optional
Tags:
Label:
uSeg EPG: false
pcTag(sclass): 5479
QoS class: Unspecified
Intra EPG Isolation: Enforced Unenforced
Custom QoS: select a value
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: Tenant1/BD4
Resolved Bridge Domain: Tenant1/BD4
Monitoring Policy: select a value
SHOW USAGE
SUBMIT
RESET

Create Device with Go-Through mode with 4 logical interfaces on Cisco APIC (“Ins” and “Out” for Service Graph 1, “g2_ins” and “g2_out” for Service Graph 2)



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation

Device Config

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. Please leave the field in this section untouched for Go-Through mode deployment.

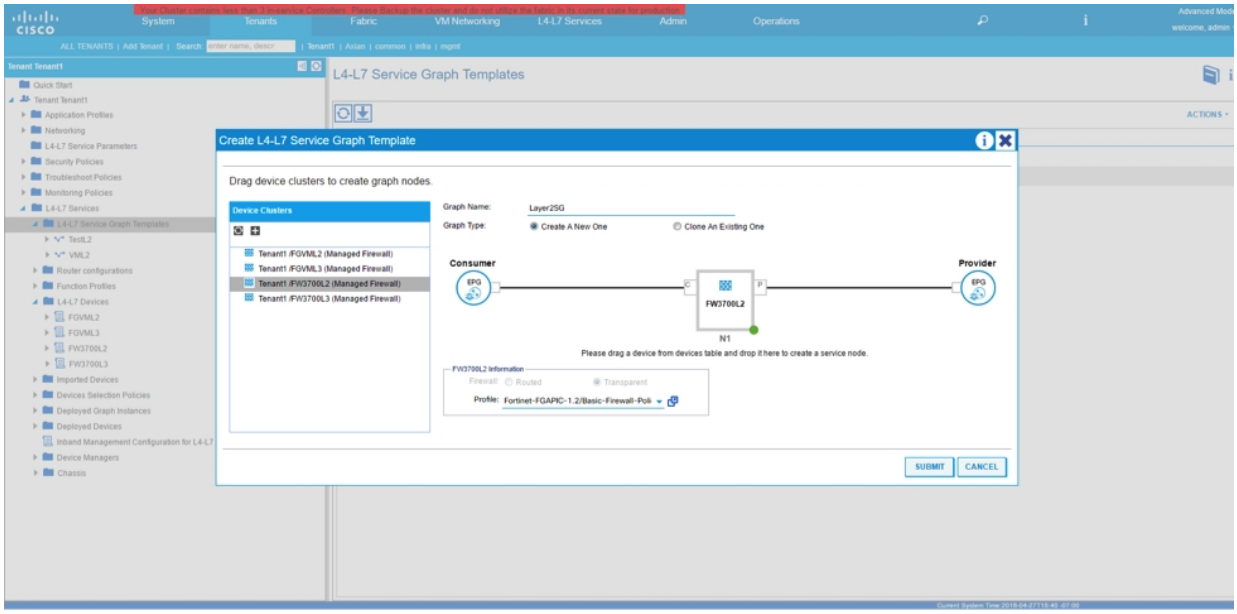
Function Config

Function Config consist of:

- **Network**
  - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
  - This folder is the container for following list of Folders:
    a. FWServiceFolder – Firewall Service Object container
    b. IPv4/IPv6 DoS Policy – Dos Policy configuration
    c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
    d. IPv4 Policy – Firewall Policy Rule container
    e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    f. ScheduleFolder – Schedule container
- **VDOM-Folder**
  - VDOM internal and external interfaces

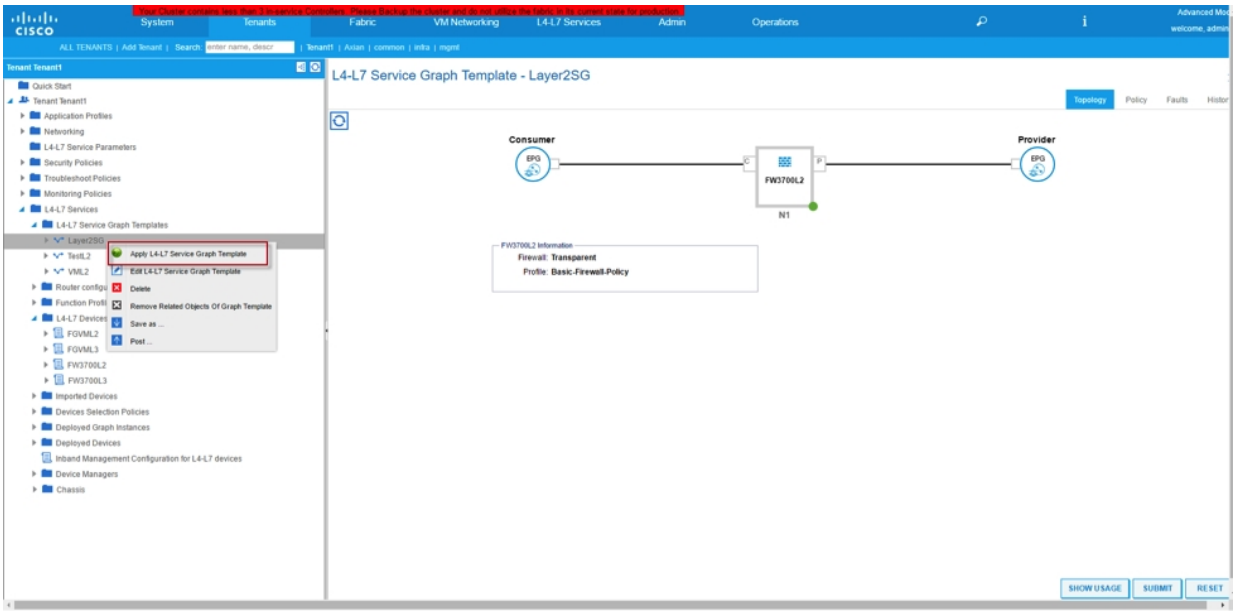
Create Service Graph1

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

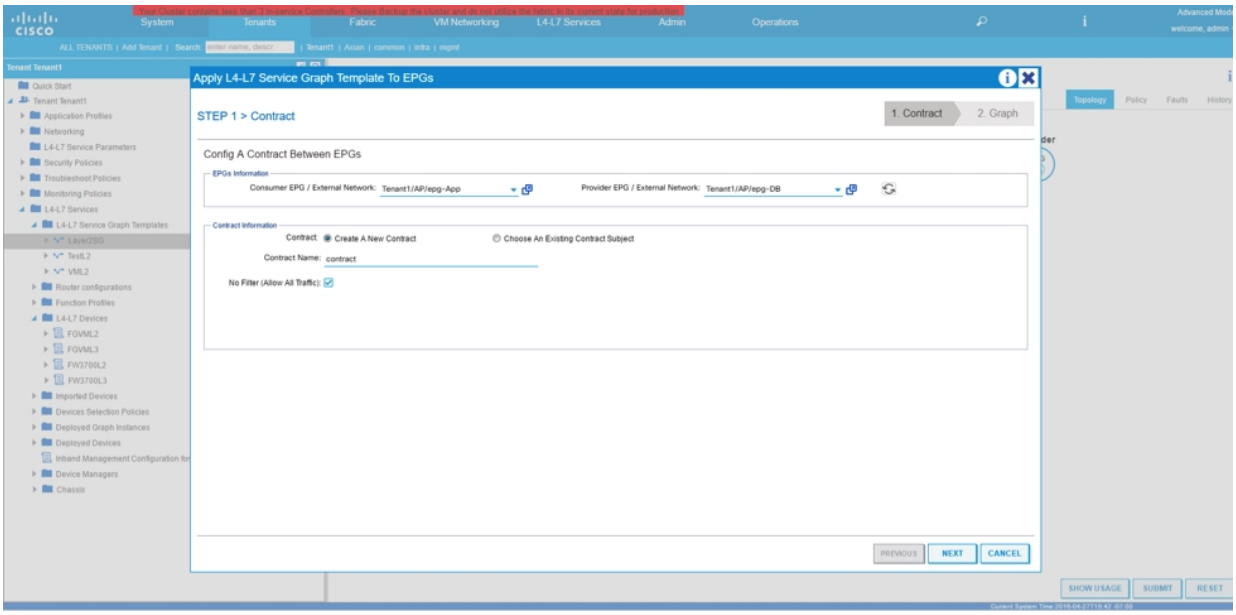


Deploy Service Graph1

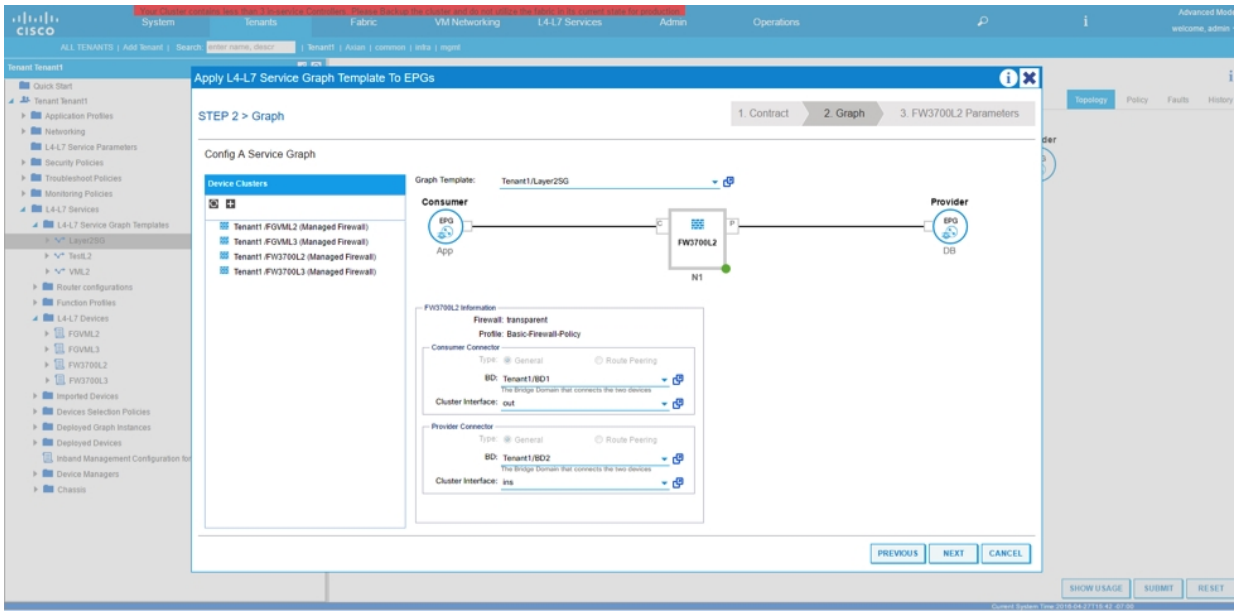
Once we combined the Firewall configuration and associated device together, we are ready to deploy Service Graph 1



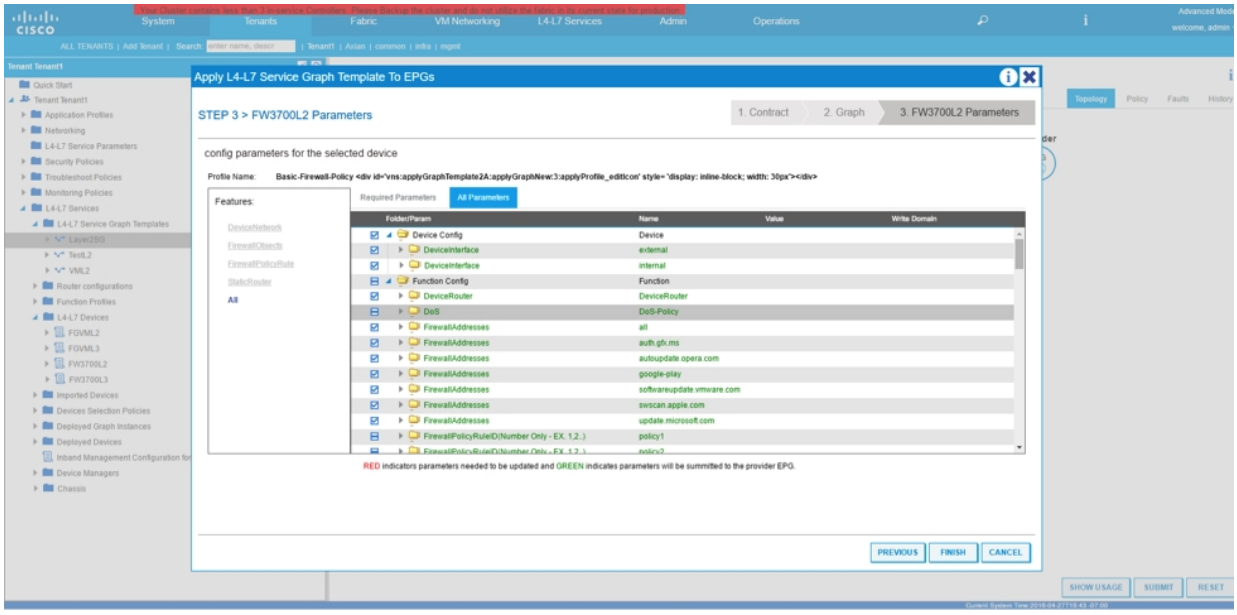
On next screen select the Consumer and provider EPGs (“Apps” and “DB”) and assign a contract name or select a pre-define contract.



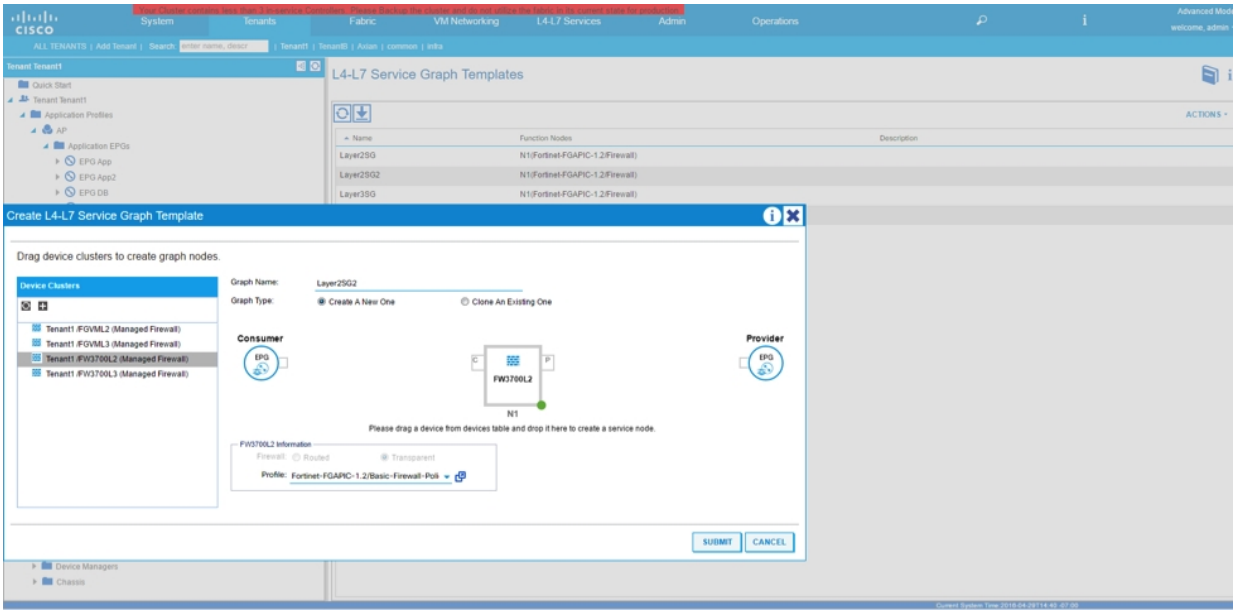
Next screen select the logical interfaces (“ins” and “out”) defined during the creation of Layer4-7 Device.



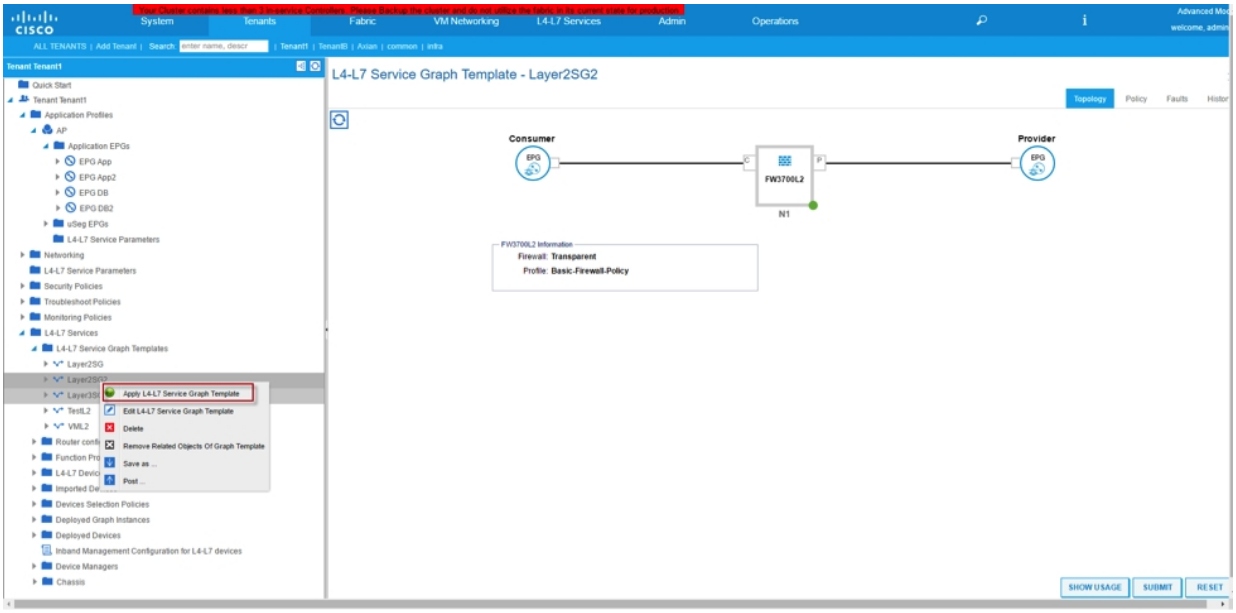
Last minute check to make sure configuration is good before hit “Finish” button



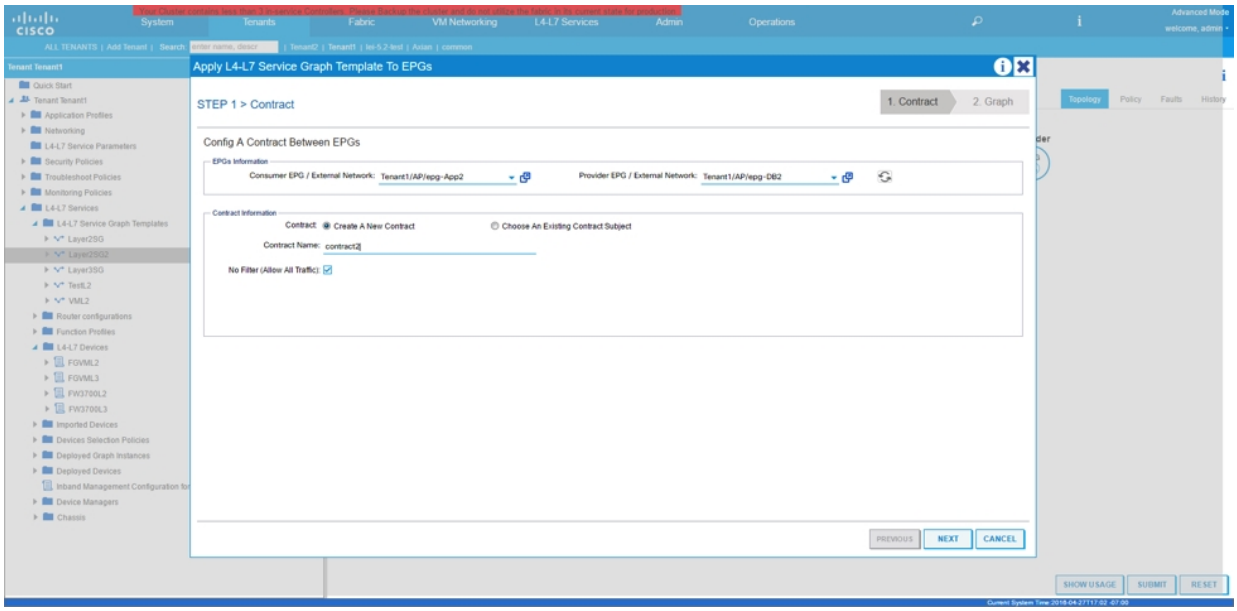
Create Service Graph2



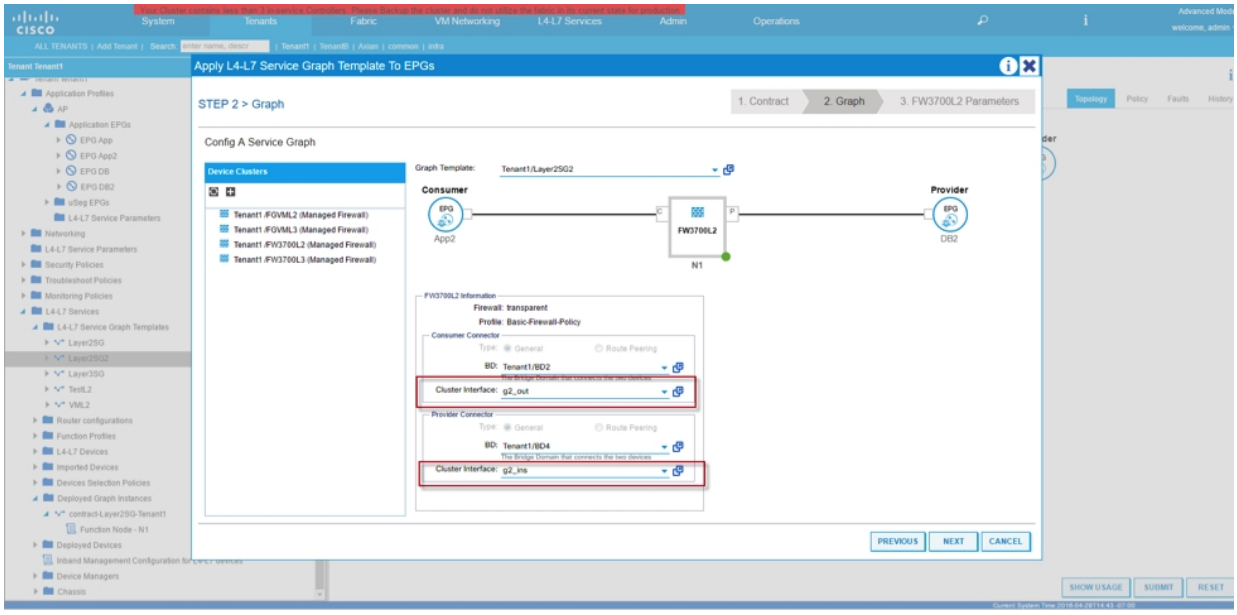
Deploy Service Graph2



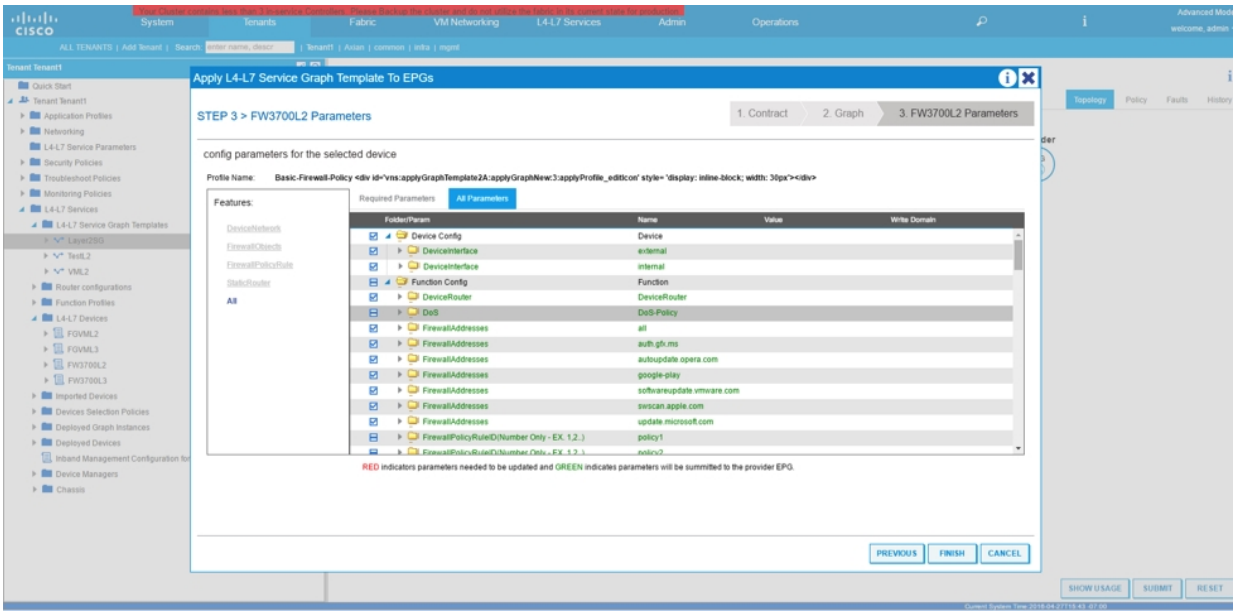
On next screen select the Consumer and provider EPGs (“Apps2” and “DB2”) and assign a contract name or select a pre-define contract.



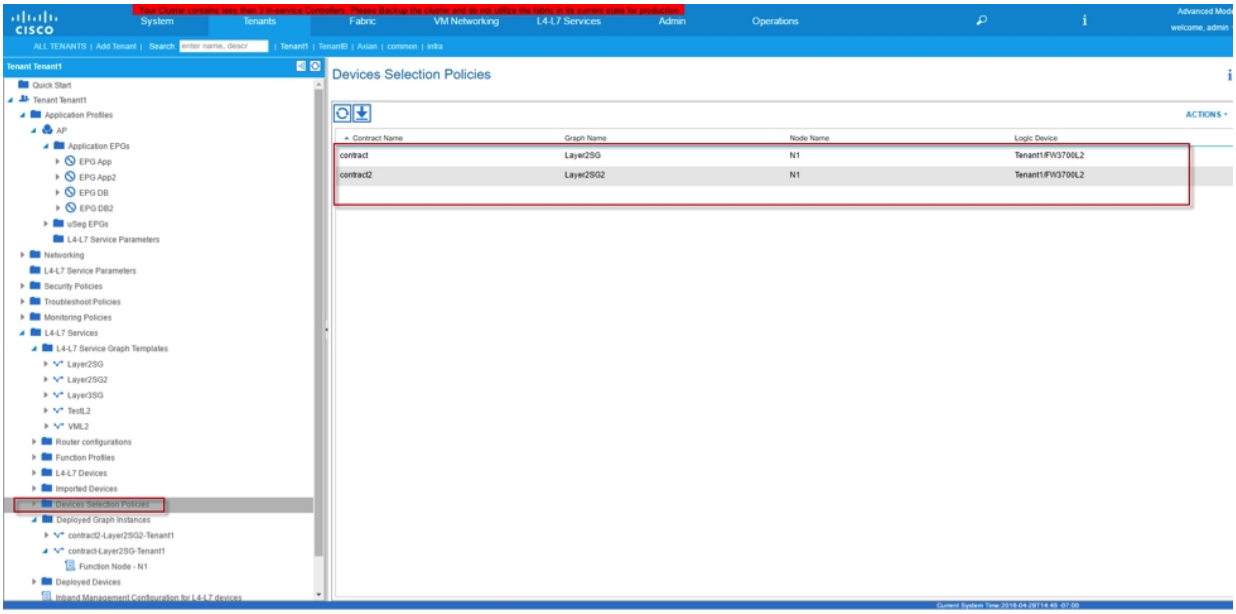
Next screen select the same logical interfaces (g2_ins and g2_out) defined during the creation of Layer 4-7 Device.



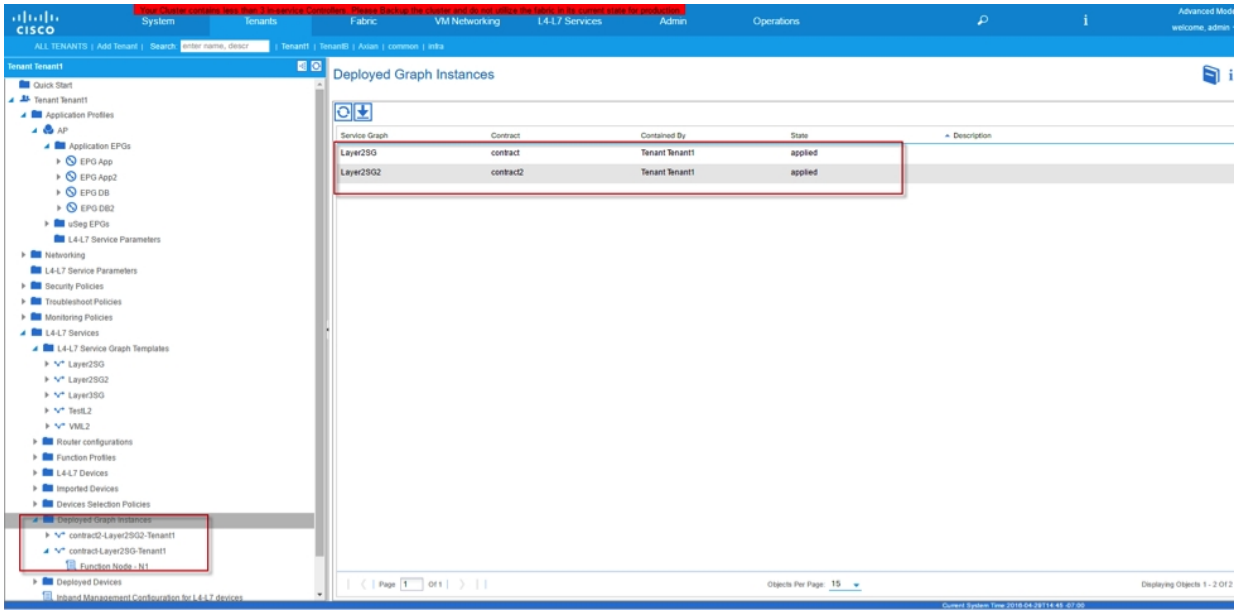
Last minute check to make sure configuration is good before hit “Finish” button

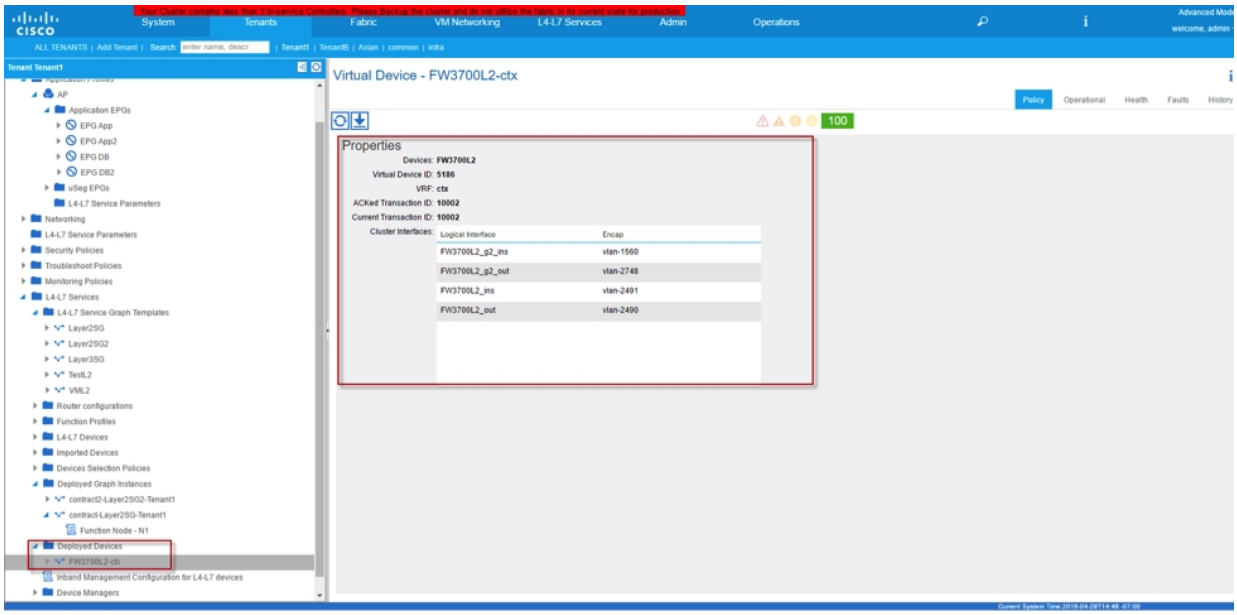


Verify Device Selection Policies Creation



Verify Service Graphs Deployment



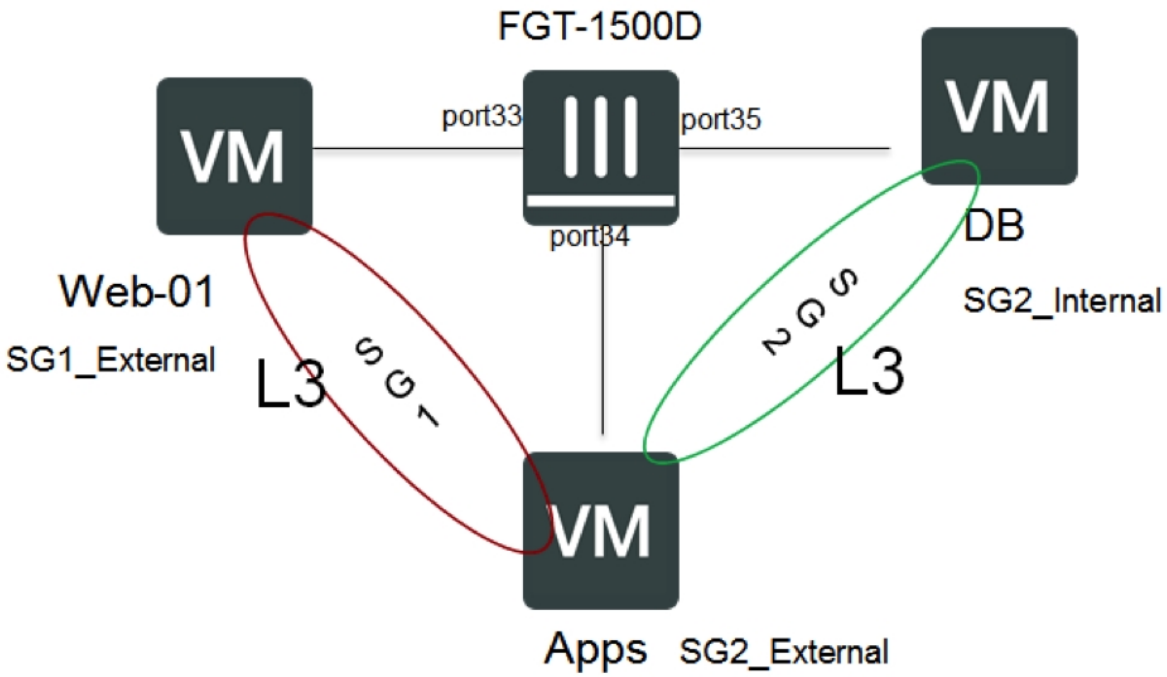


Deploy the firewall device with shared interfaces through multiple service graphs

Pre-requisite

- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- Layer4-7 Device Package has imported into Cisco APIC

Basic Topology



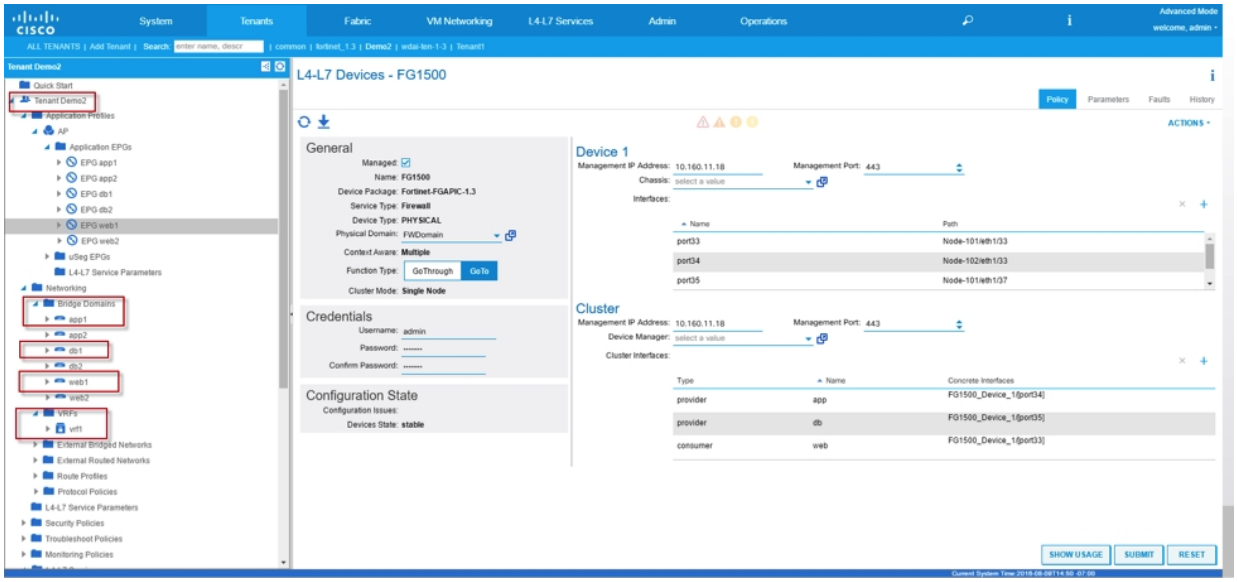
Work Flow:

1. Create Tenant (“Demo2” in our example)
2. Create VRF (“vrf1” in our example)
3. Create 3 Bridge Domains (“Web1”, “App1”, and “DB1” in our example)
4. Associate Bridge Domains to VRF

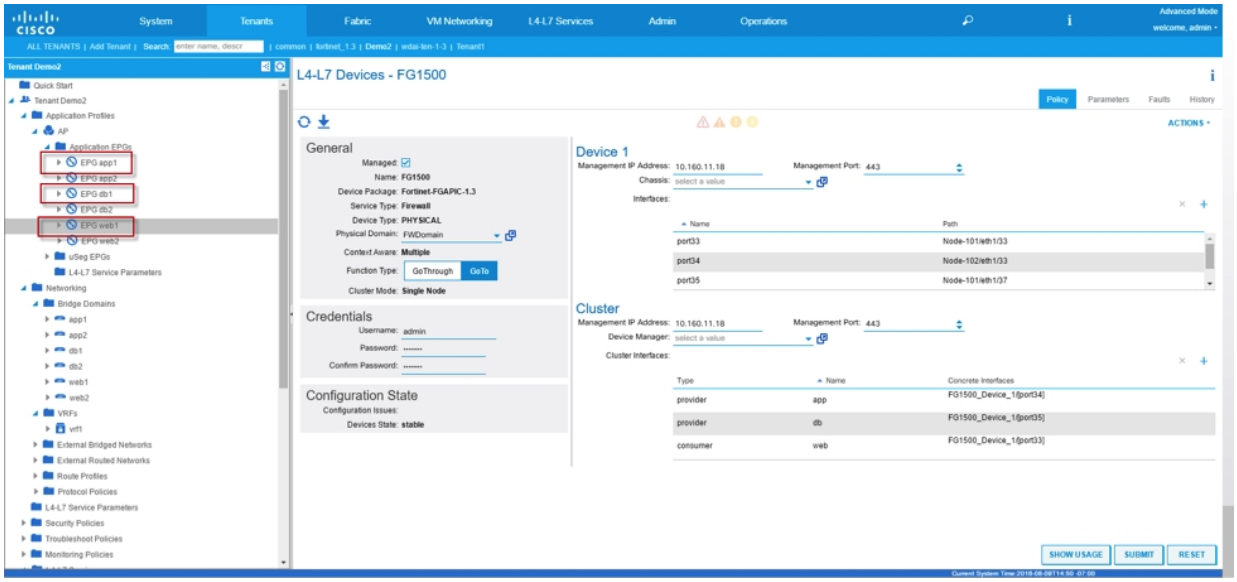
5. Create 3 EPGs (“Web1” , “App1”, and “DB1” in our example)
6. Associate EPGs to Bridge Domains (EPG “Web1”, “App1”, and “DB1” are mapped to Bridge Domain “Web1”, “App1”, and “DB1” respectively in our example)
7. Create Go-To mode Device on Cisco APIC and define 3 logical interfaces
8. Create Functional Profile
9. Create 2 Service Graph Templates
10. Deploy Service Graph 2 times on the same device but with different EPG pairs

Configuration

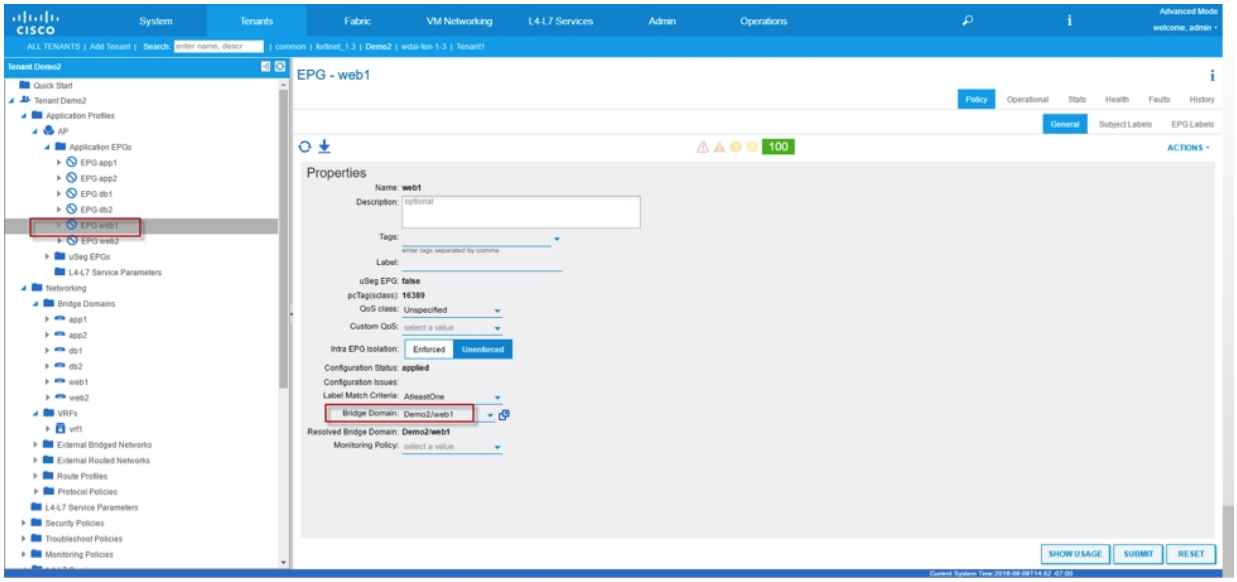
Create Tenant, VRF and 3 Bridge Domains on Cisco APIC

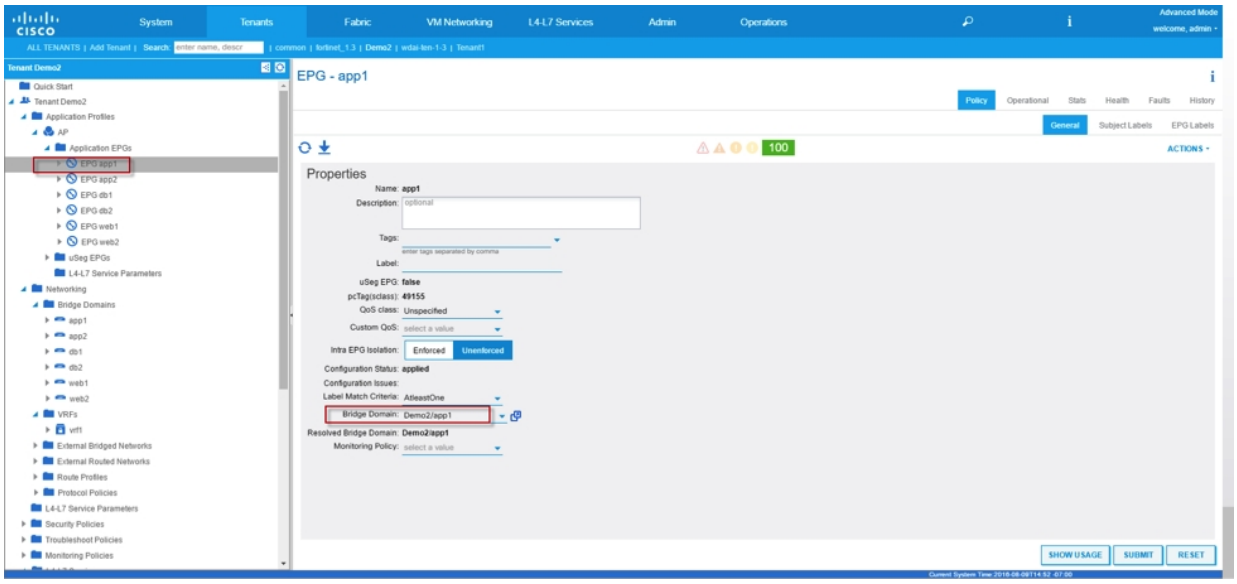


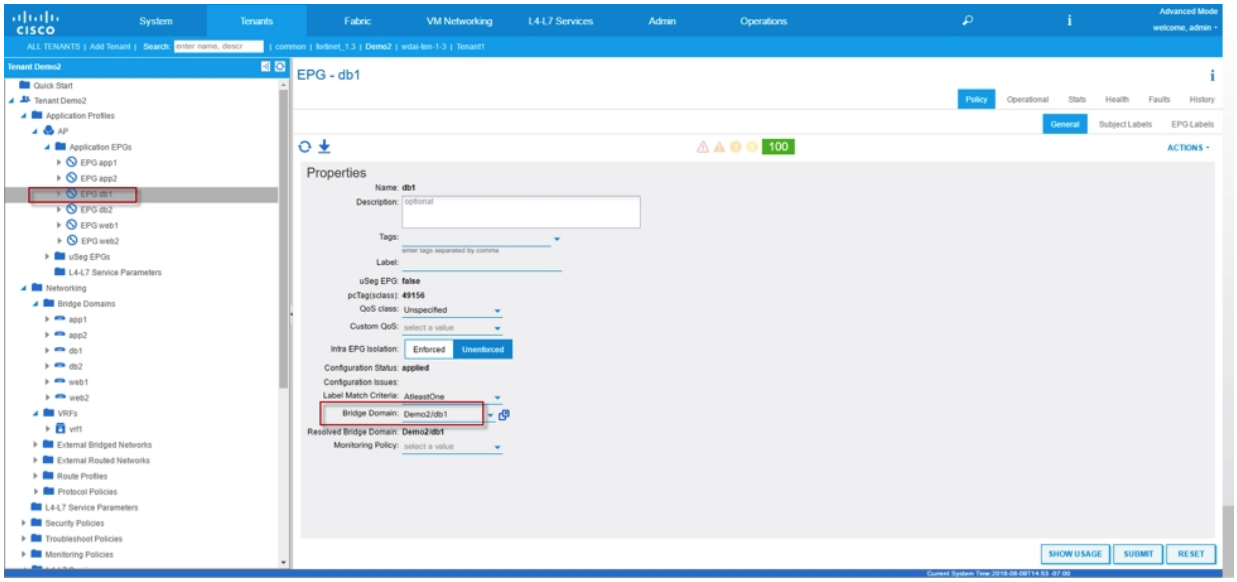
Create 3 EPGs



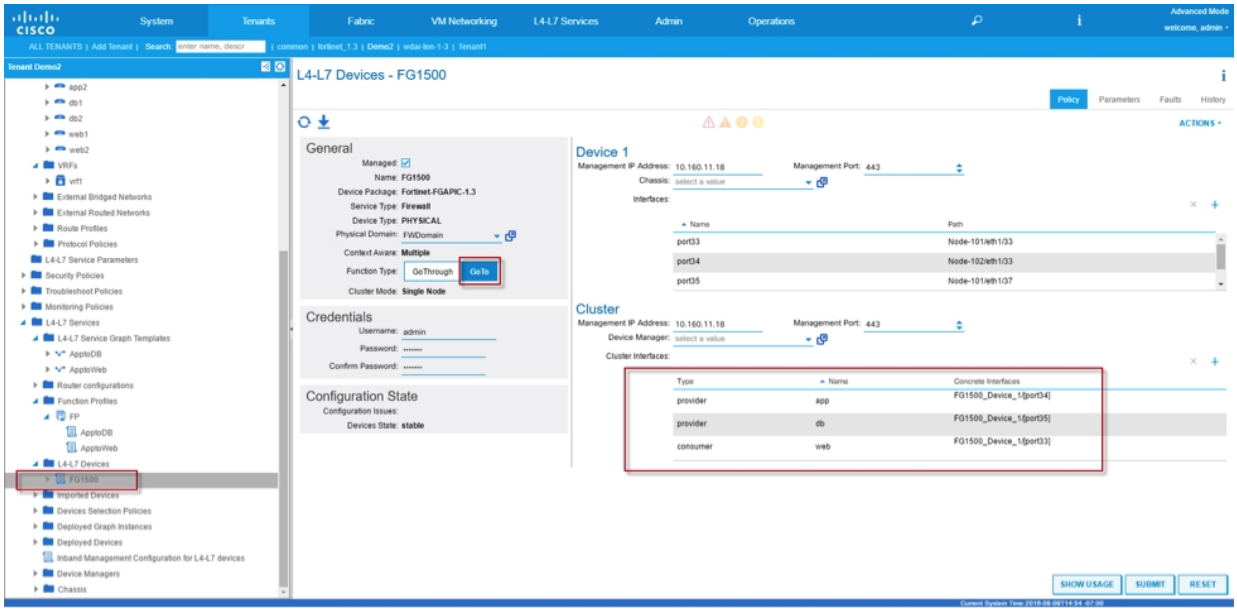
Associate EPG “Web1”, “App1”, and “DB1” to Bridge Domain “Web1”, “App1”, and “DB1” respectively




System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Tenant Demo2
EPG - app1
Properties
Name: app1
Description: optional
Tags:
Label:
uSeg EPG: false
pcTag(sclass): 49155
QoS class: Unspecified
Custom QoS:
Intra EPG Isolation: Enforced Unenforced
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: Demo2/app1
Resolved Bridge Domain: Demo2/app1
Monitoring Policy:
SHOW USAGE
SUBMIT
RESET

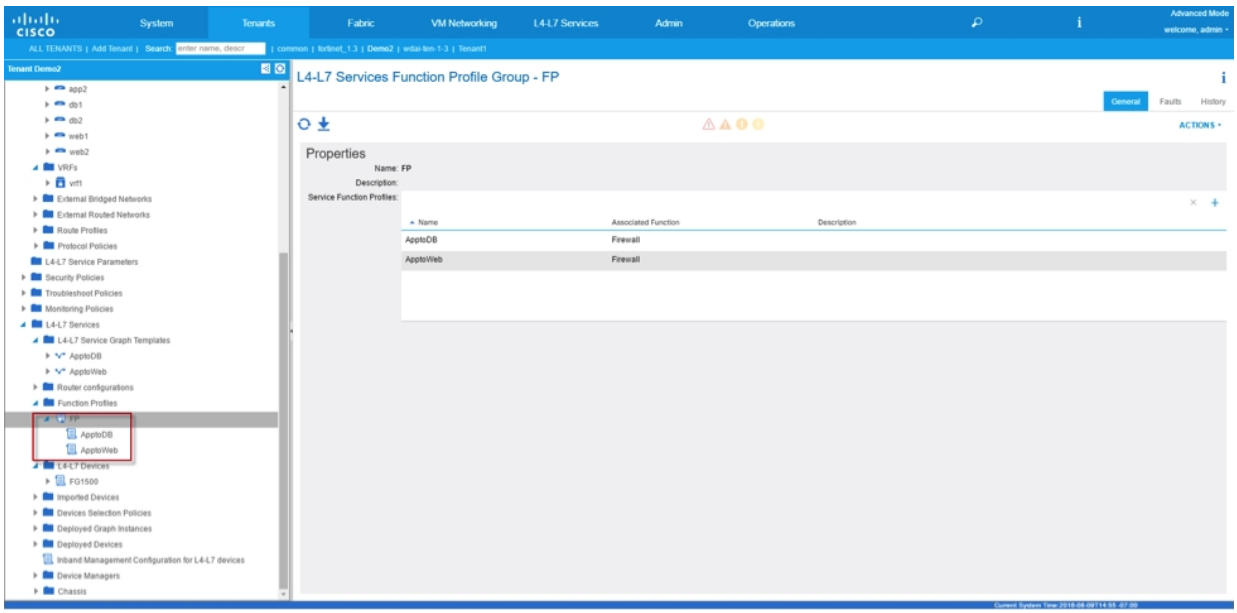

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Tenant Demo2
EPG - db1
Properties
Name: db1
Description: optional
Tags:
Label:
uSeg EPG: false
pcTag(sclass): 49156
QoS class: Unspecified
Custom QoS:
Intra EPG Isolation: Enforced Unenforced
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: Demo2/db1
Resolved Bridge Domain: Demo2/db1
Monitoring Policy:
SHOW USAGE
SUBMIT
RESET

Create Device with Go-To mode with 3 logical interfaces on Cisco APIC (“Web” “App” and “DB”)



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation:

Device Config

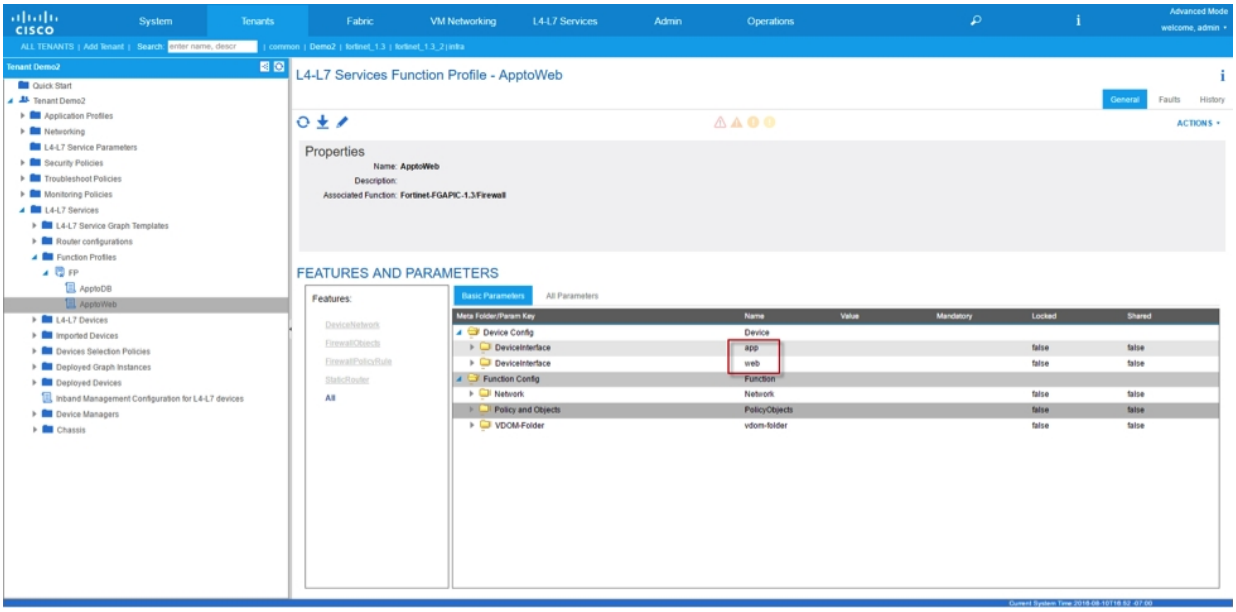
Contains External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. Please leave the field in this section untouched for Go-Through mode deployment.

Function Config

Function Config consist of:

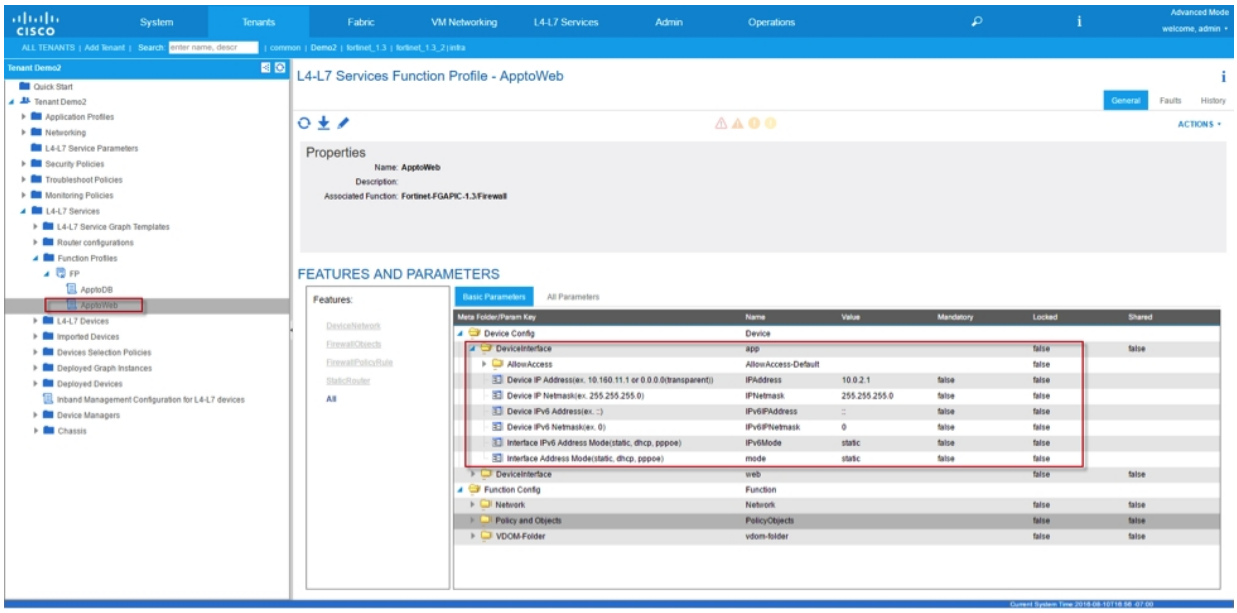
- **Network**
  - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
  - This folder is the container for following list of Folders:
    a. FWServiceFolder – Firewall Service Object container
    b. IPv4/IPv6 DoS Policy – Dos Policy configuration
    c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
    d. IPv4 Policy – Firewall Policy Rule container
    e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    f. ScheduleFolder – Schedule container
- **VDOM-Folder**
  - VDOM internal and external interfaces

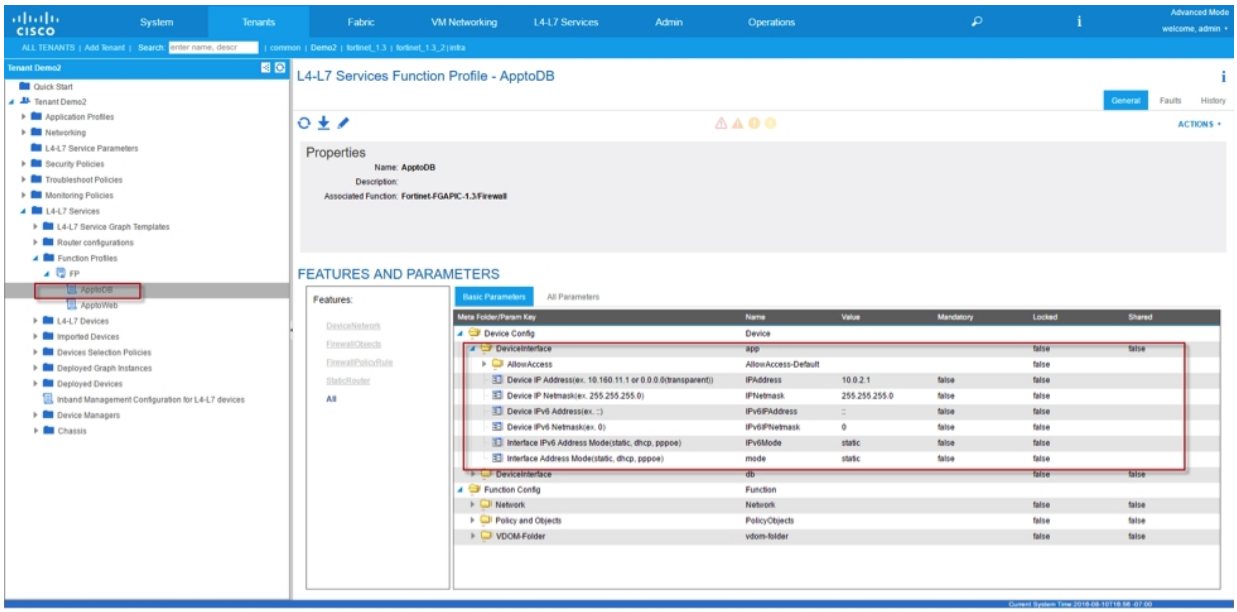
Beginning with this release, we allow the change of DeviceInterface name and the default is External/Internal. Please see below screenshot where we changed the DeviceInterface name from External/Internal to app/web respectively.



In addition, for this use case scenario, App is going to be the shared interface between the two service graphs, therefore it is crucial that the DeviceInterface name and the content are identical across both service graphs.

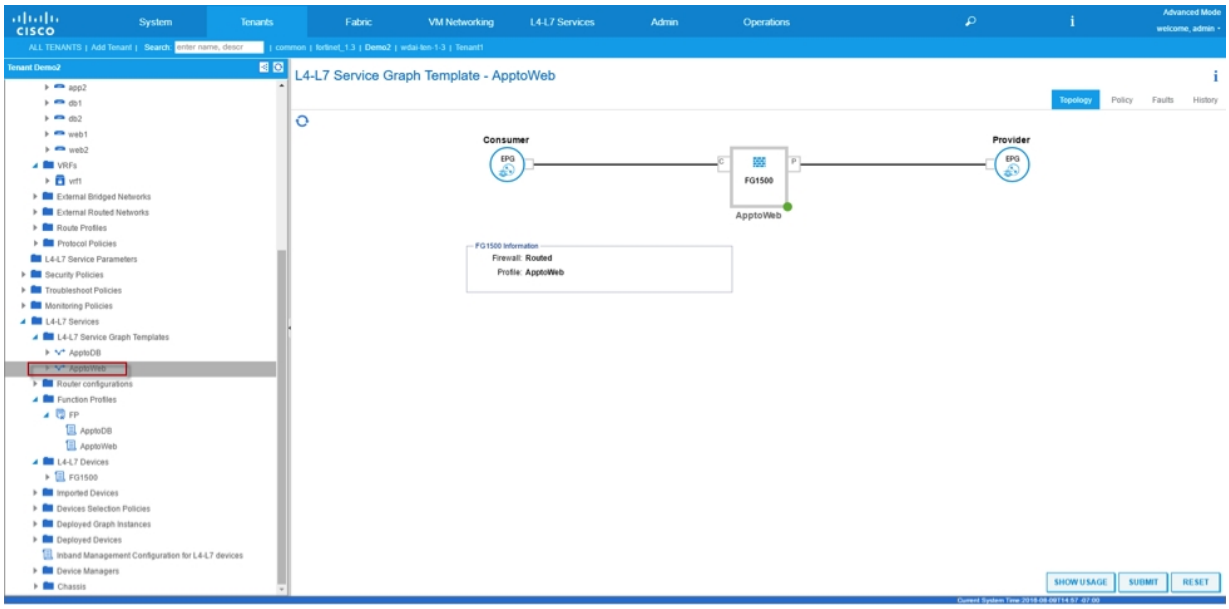
Please see screenshot for “app” between two service graphs (ApptoWeb and ApptoDB).





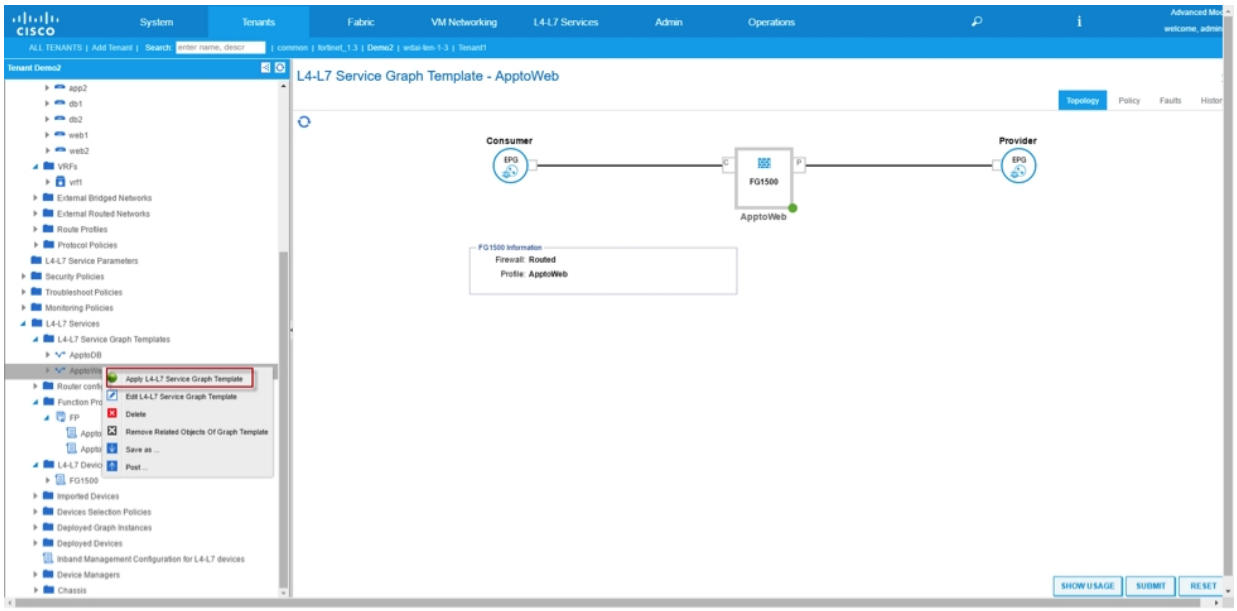
Create Service Graph1 for Web1 and App1

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

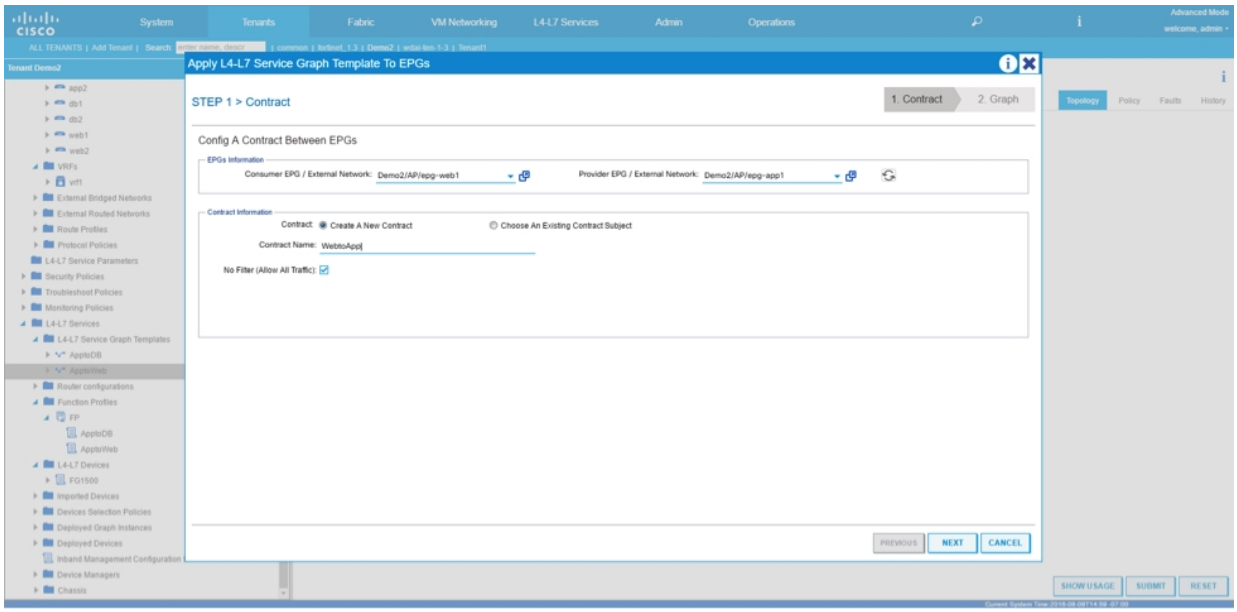


Deploy Service Graph1 Web1 to App1

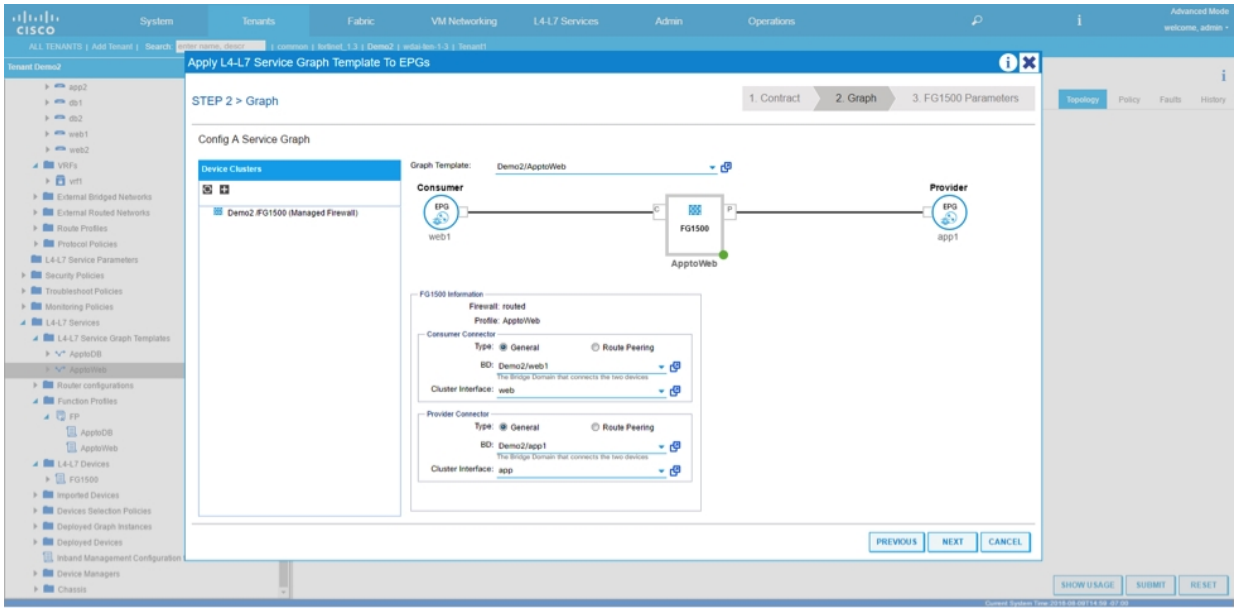
Once we combined the Firewall configuration and associated device together, we are ready to deploy Service Graph 1



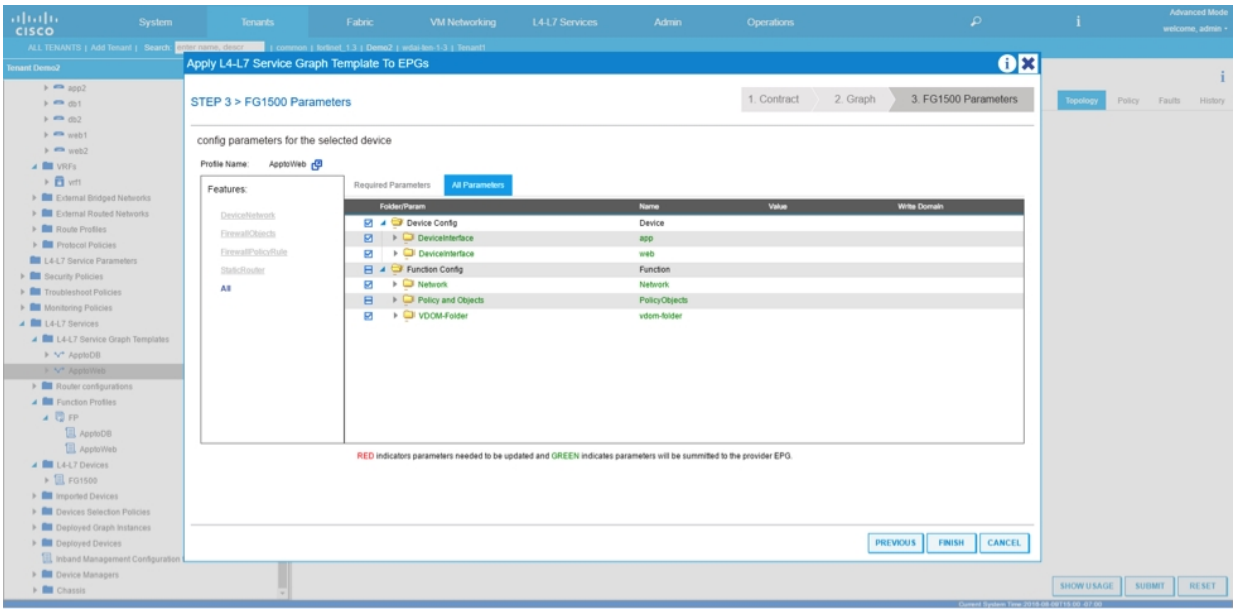
On next screen select the Consumer and provider EPGs (“Web1” and “App1”) and assign a contract name or select a pre-define contract.



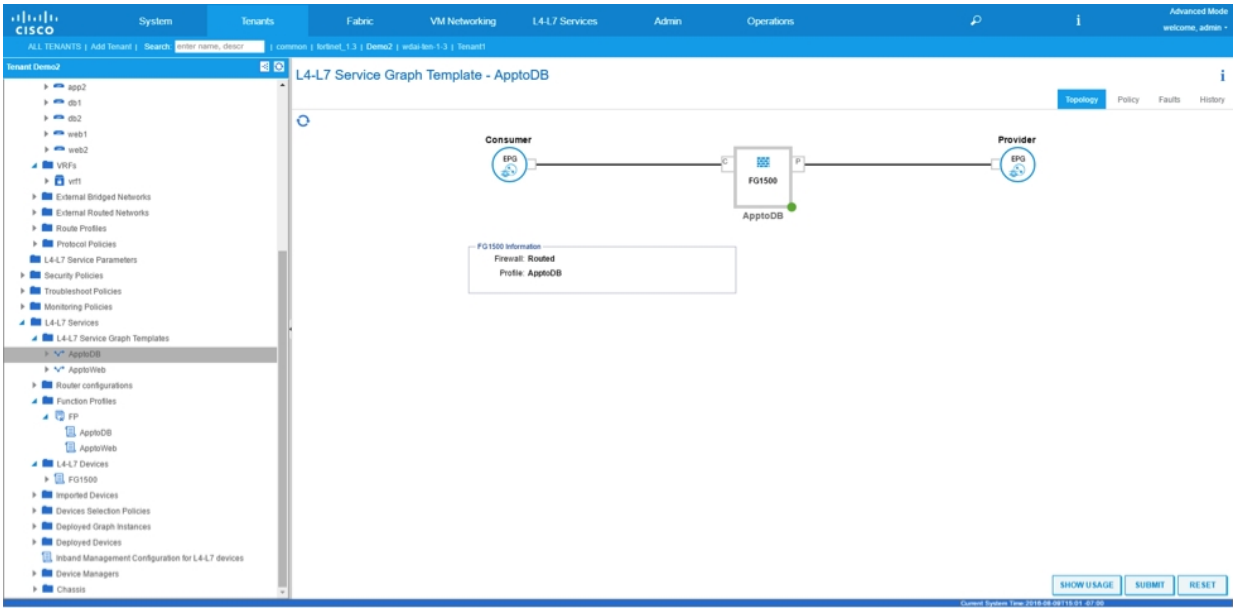
Next screen select the logical interfaces (“app” and “web”) defined during the creation of Layer4-7 Device.



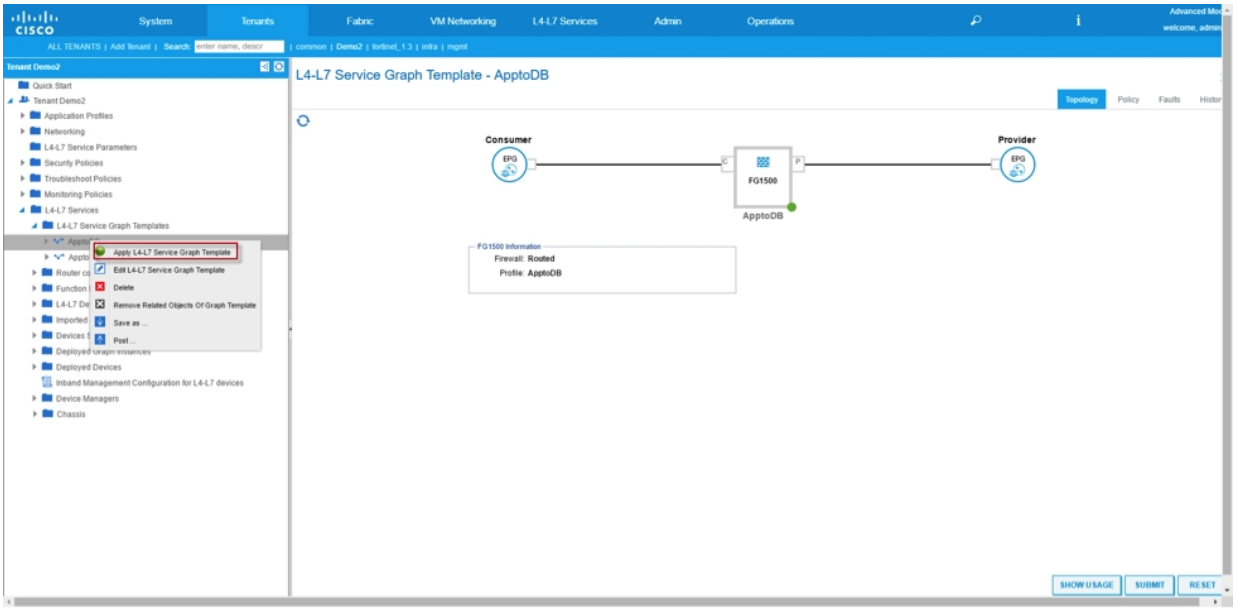
Last minute check to make sure configuration is good before hit “Finish” button



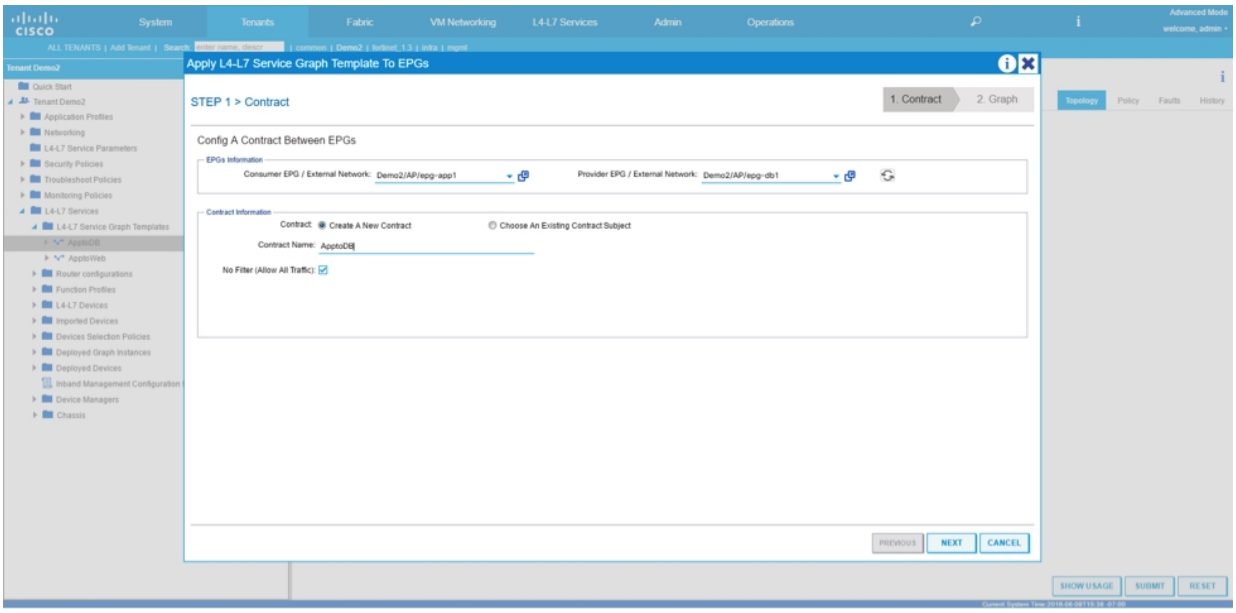
Create Service Graph2 App1 to DB1



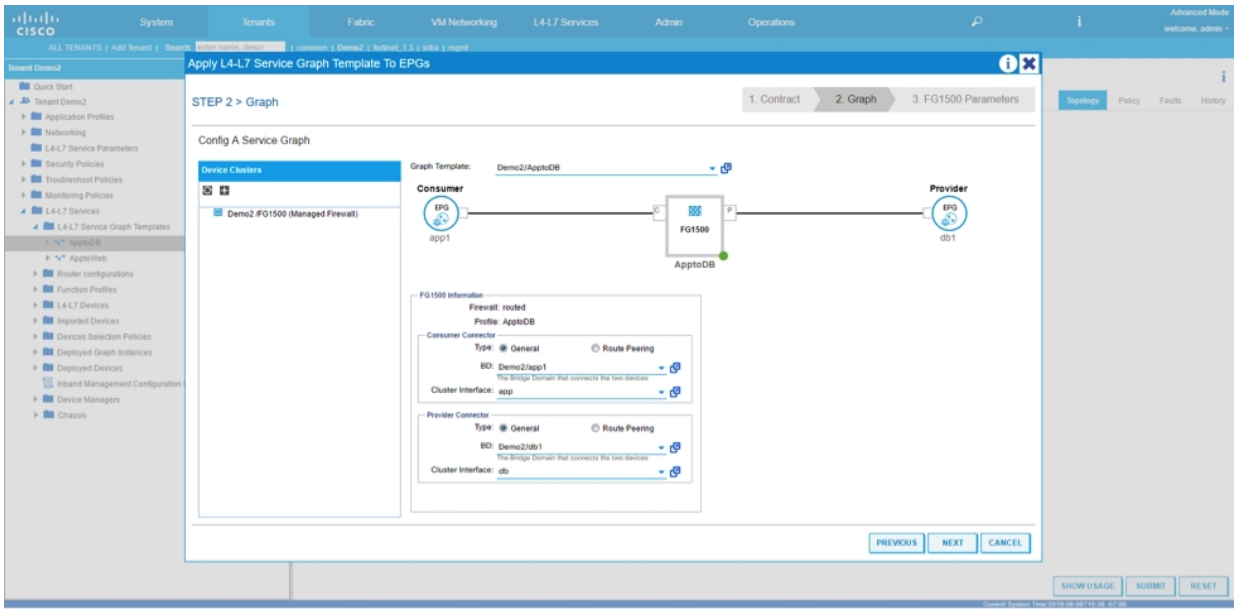
Deploy Service Graph2 App1 to DB1



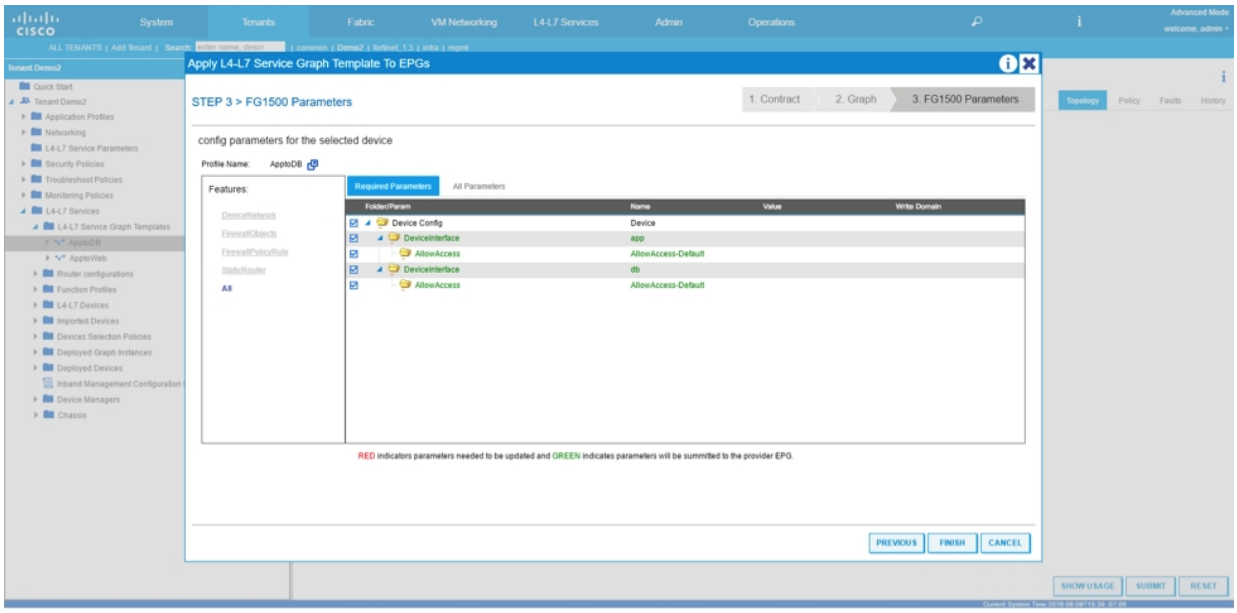
On next screen select the Consumer and provider EPGs (“App1” and “DB1”) and assign a contract name or select a pre-define contract.



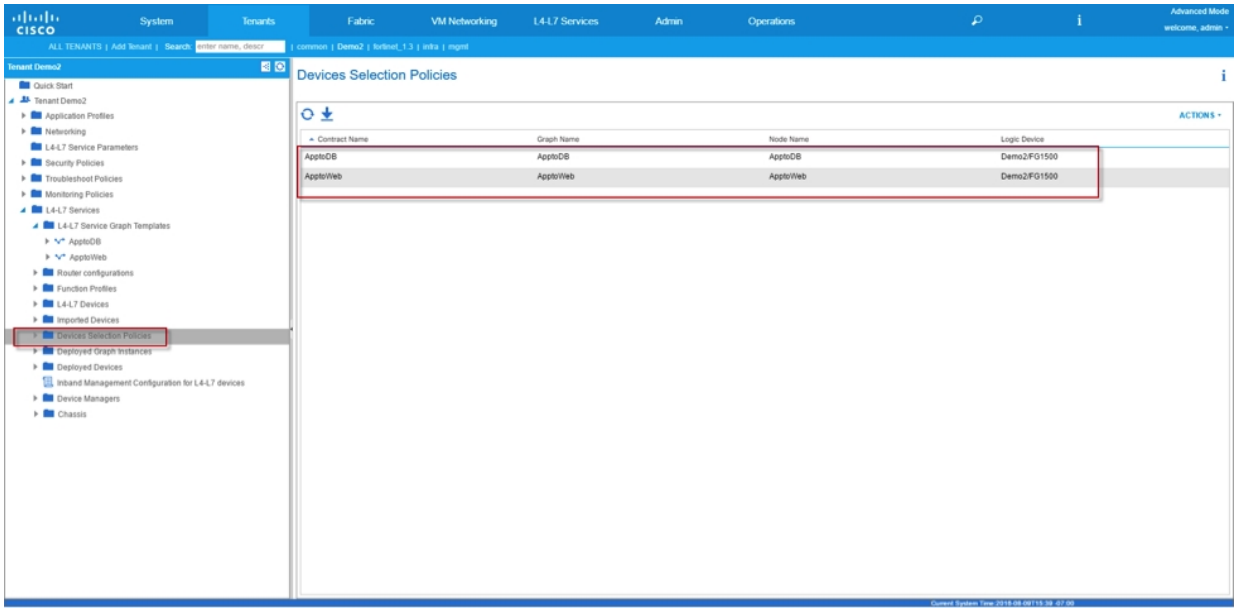
Next screen select the logical interfaces (App and DB) defined during the creation of Layer4-7 Device.



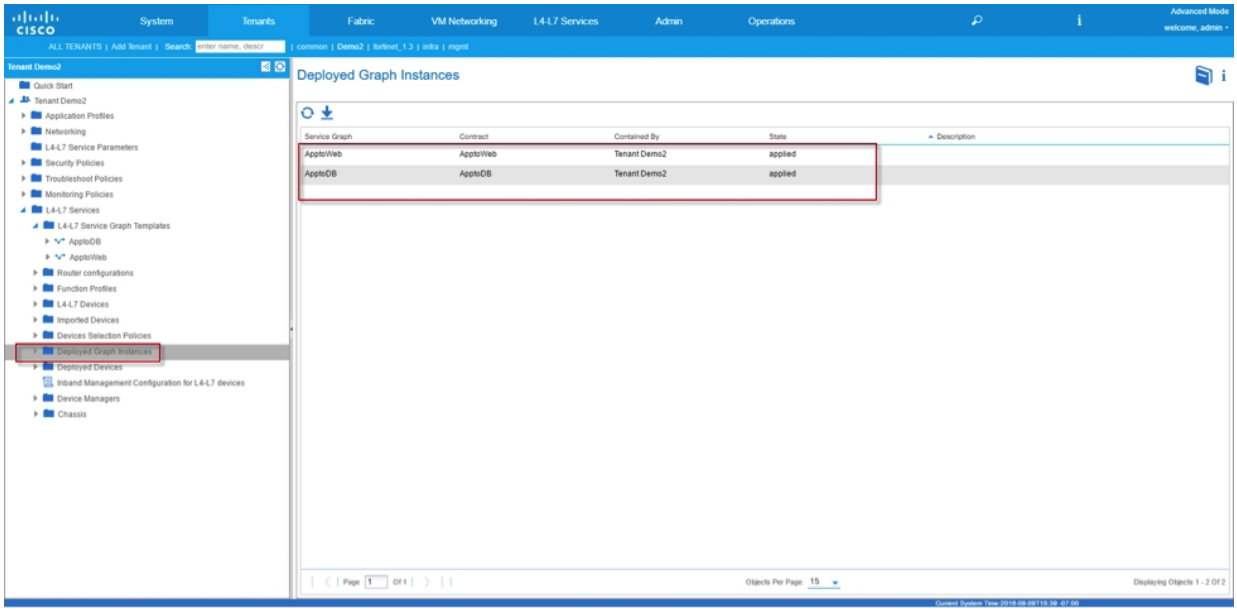
Last minute check to make sure configuration is good before hit “Finish” button

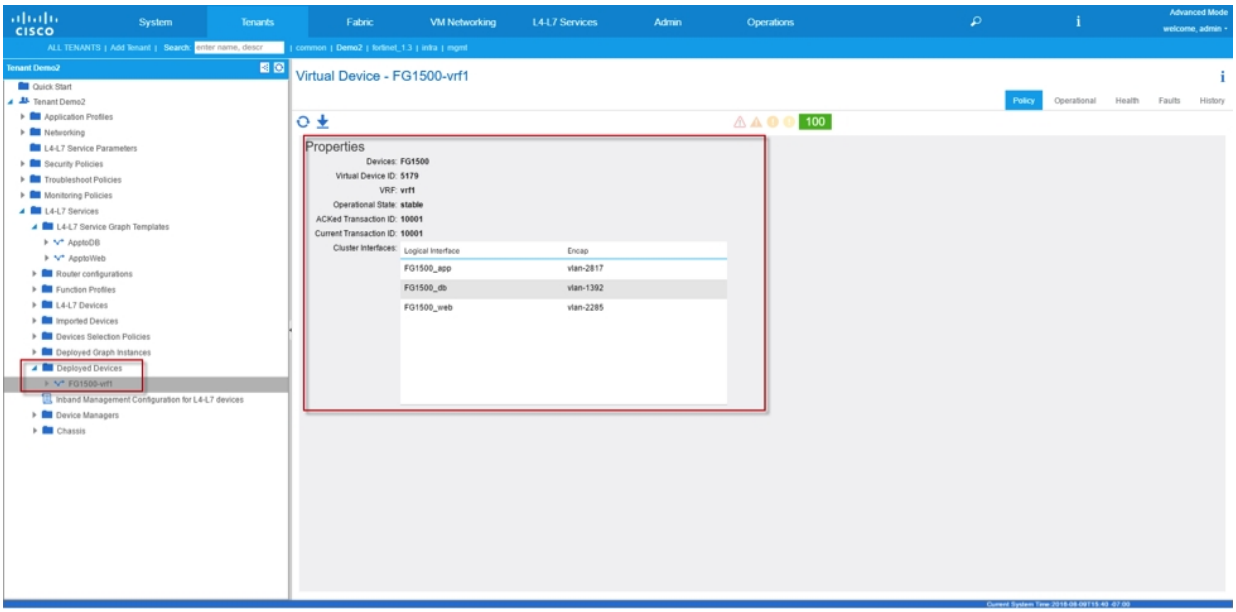


Verify Device Selection Policies Creation



Verify Service Graphs Deployment





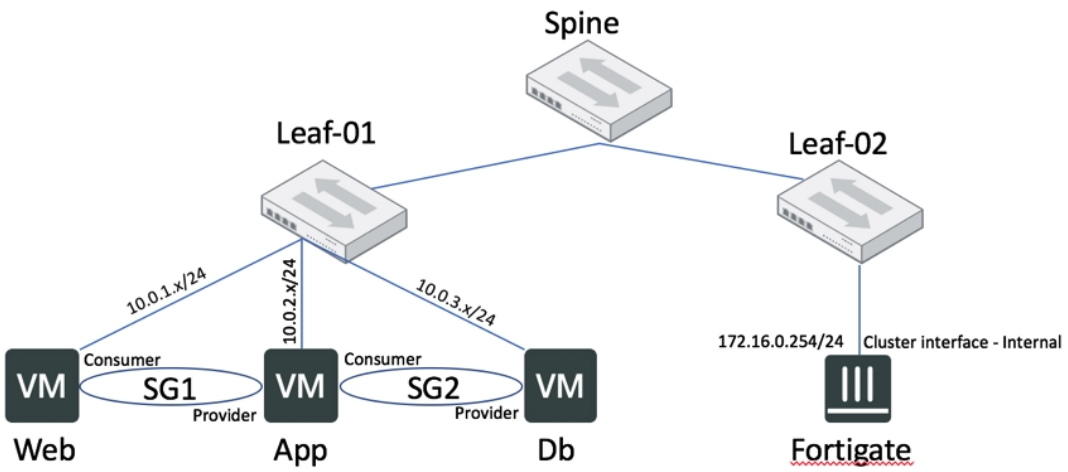
Deploy the firewall device in a one-arm configuration with policy based redirect

Prerequisites

- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- Layer 4-7 Device Package has been imported into Cisco APIC
- Layer 4-7 Policy Based Redirect required (Cisco ACI 2.x above)
- Dynamic EPG Notification (optional)
- Separate Firewall Bridge Domain. Required for Policy Based Redirect

For N9K93128TX, N9K9396PX, and N9K9396TX switches, the service appliance must not be in the same leaf switch as either the source or destination endpoint group.

Basic Topology

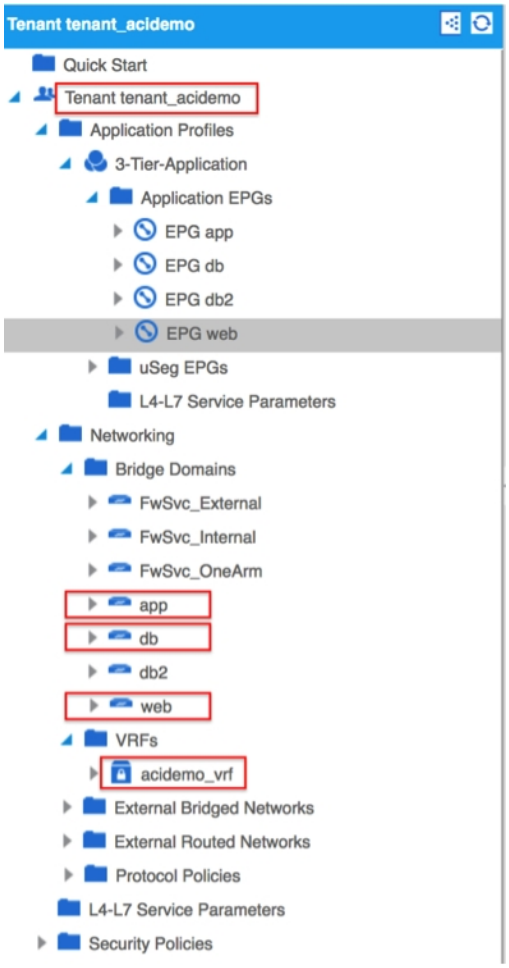


Work Flow:

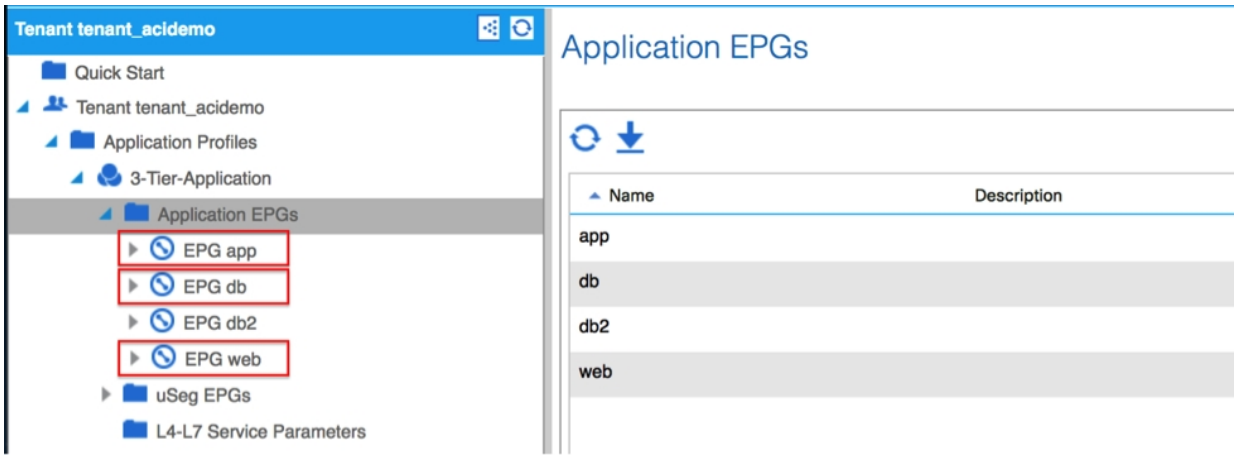
1. Create Tenant (“acidemo” in our example)
2. Create VRF (“acidemo_vrf” in our example)
3. Create 3 Bridge Domains (“web”, “app”, and “db” in our example)
4. Associate Bridge Domains to VRF
5. Create 3 EPGs (“web”, “app”, and “db” in our example)
6. Associate EPGs to Bridge Domains (EPG “web”, “app”, and “db” are mapped to Bridge Domain “web, “app”, and “db” respectively in our example)
7. Create Dedicated Firewall Services Bridge Domain and Subnet on Cisco APIC
8. Create L4-L7 Policy Based Redirect on Cisco APIC
9. Create Go-To mode Device on Cisco APIC and define 2 logical interfaces
10. Create Functional Profile
11. Create Service Graph Template
12. Deploy Service Graph Template

Configuration

Create Tenant, VRF and 3 Bridge Domains on Cisco APIC

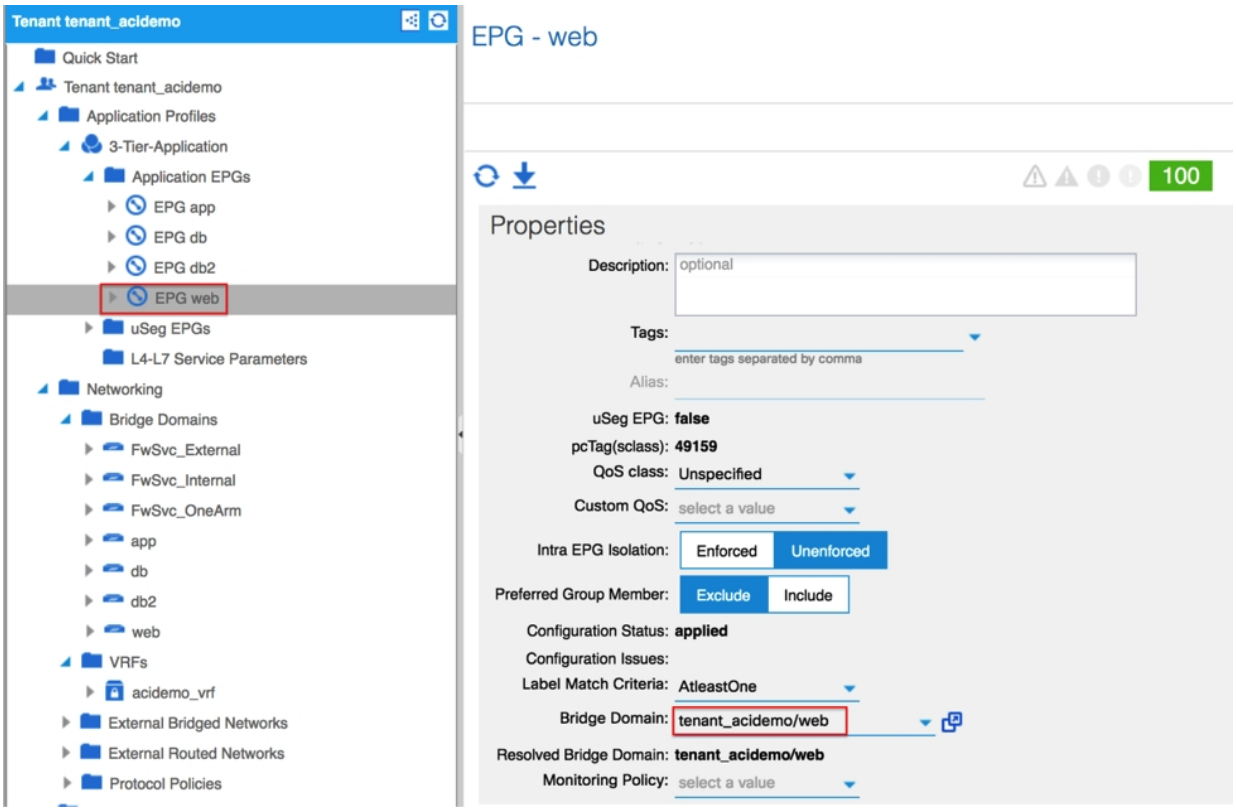


Create 3 EPGs

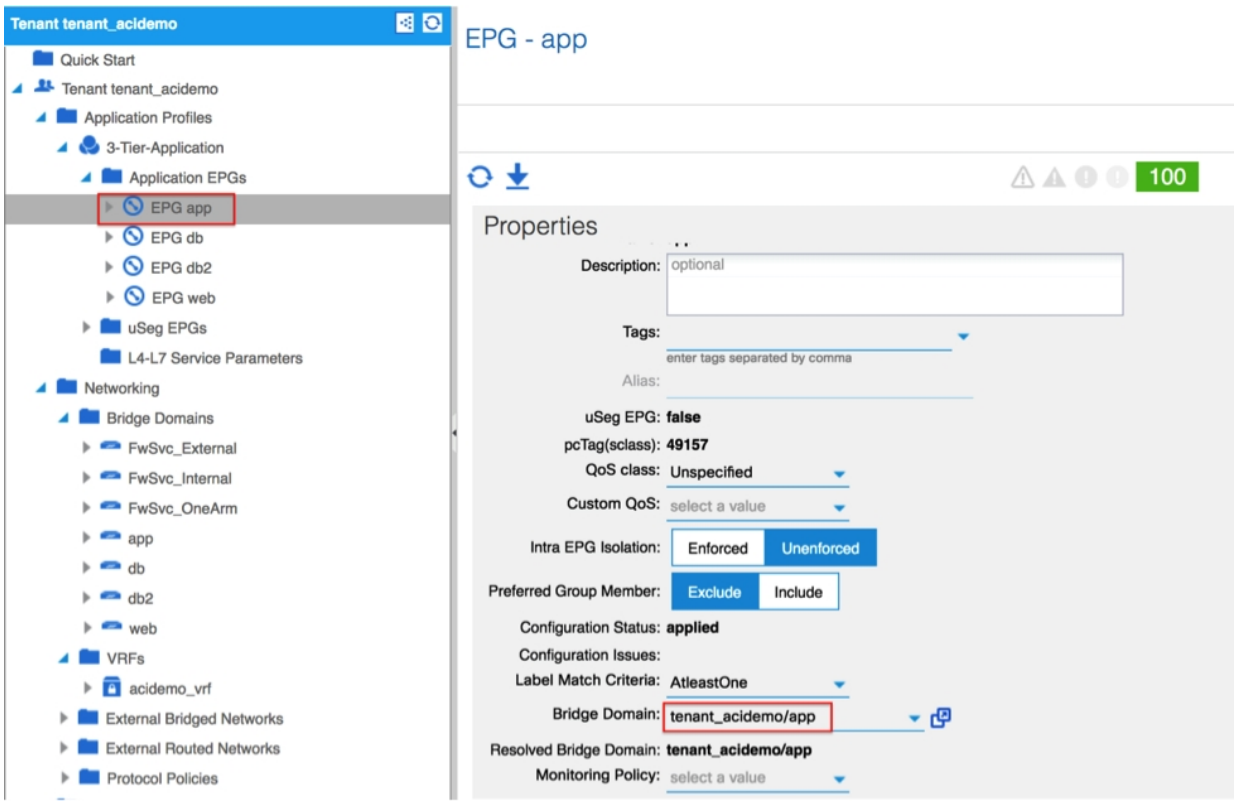


Associate EPG “web”, “app”, and “db” to Bridge Domain “web”, “app”, and “db” respectively

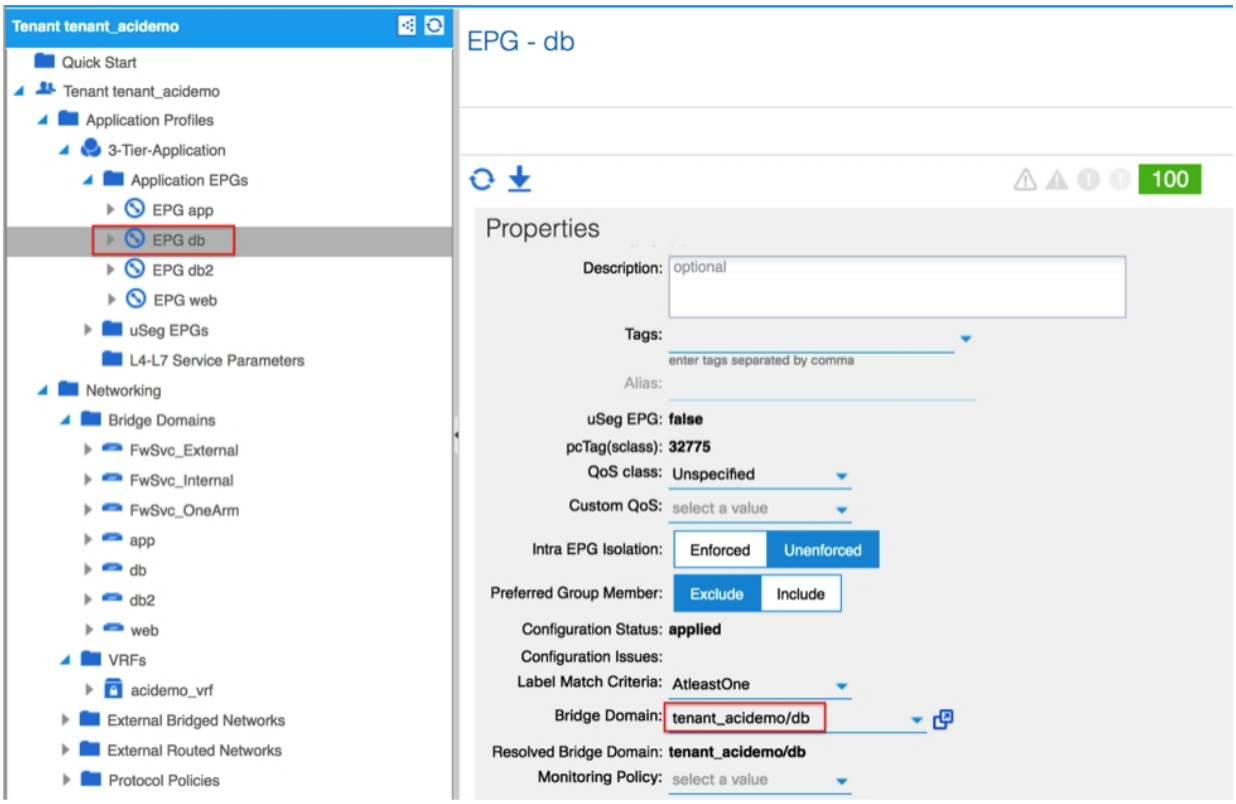
Web



App

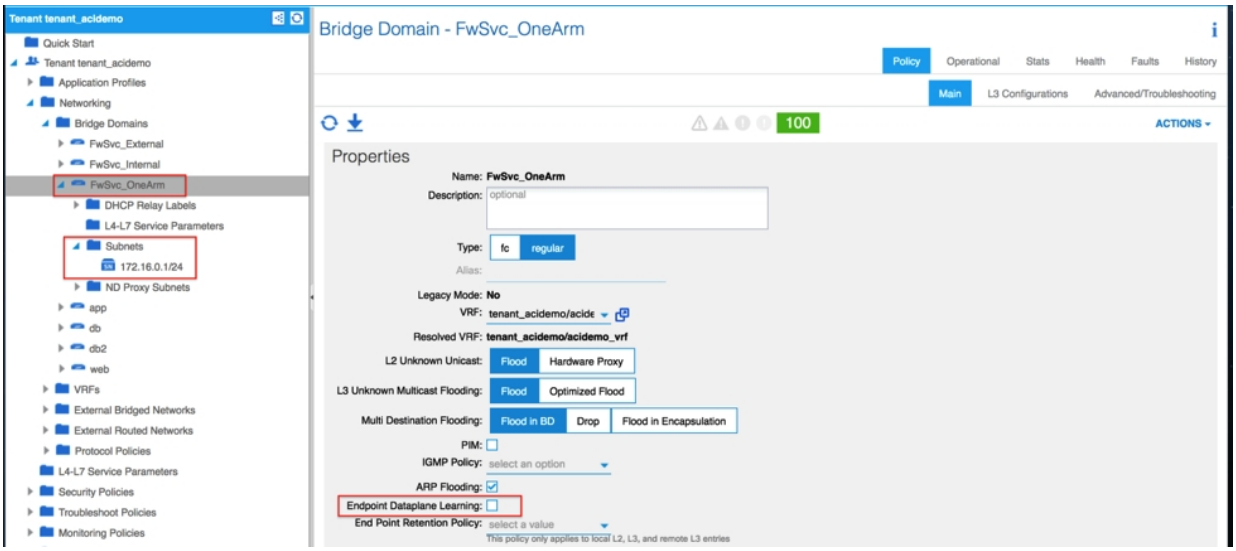

Tenant tenant_acidemo
Quick Start
Tenant tenant_acidemo
Application Profiles
3-Tier-Application
Application EPGs
EPG app
EPG db
EPG db2
EPG web
uSeg EPGs
L4-L7 Service Parameters
Networking
Bridge Domains
FwSvc_External
FwSvc_Internal
FwSvc_OneArm
app
db
db2
web
VRFs
acidemo_vrf
External Bridged Networks
External Routed Networks
Protocol Policies
EPG - app
100
Properties
Description: optional
Tags:
enter tags separated by comma
Alias:
uSeg EPG: false
pcTag(sclass): 49157
QoS class: Unspecified
Custom QoS: select a value
Intra EPG Isolation: Enforced Unenforced
Preferred Group Member: Exclude Include
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: tenant_acidemo/app
Resolved Bridge Domain: tenant_acidemo/app
Monitoring Policy: select a value

DB



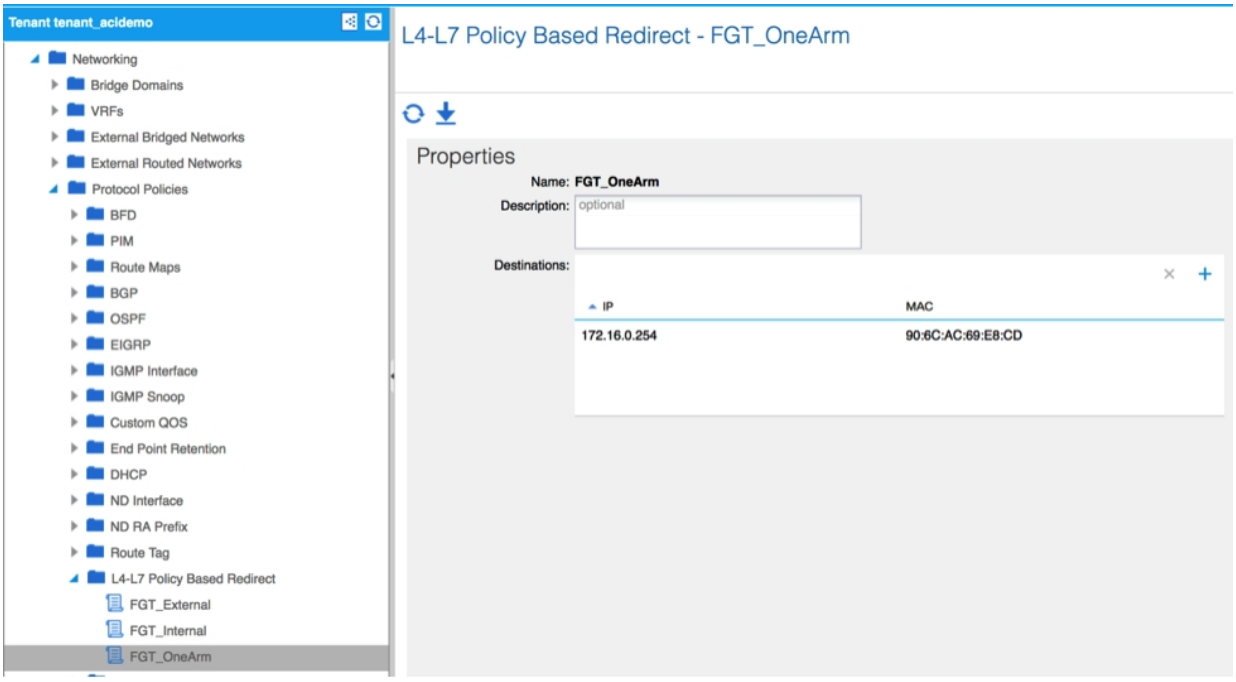
Create Dedicated Firewall Services Bridge Domain and Subnet on Cisco APIC

Uncheck Endpoint Dataplane Learning and Create a Subnet. This Subnet IP will be used later in the default route on the Fortigate.



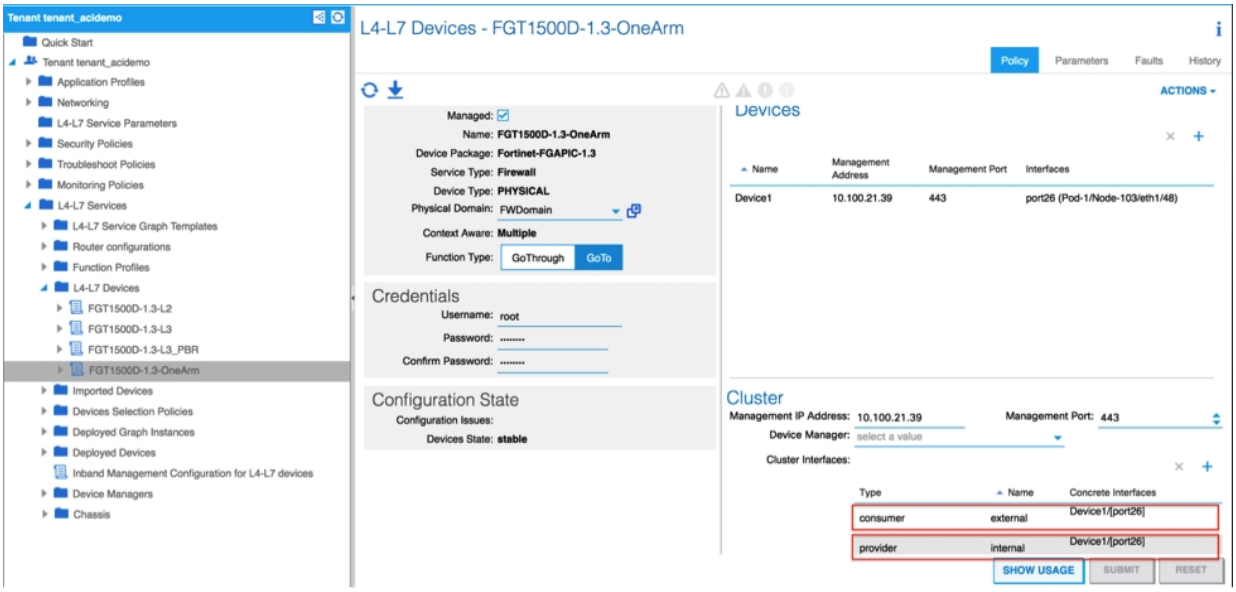
Create L4-L7 Policy Based Redirect on Cisco APIC

The IP Address will be the same IP assigned to the Fortigate internal interface later. The MAC Address is the same as the physical interface MAC on the Fortigate. This can be obtained with global Fortigate CLI command “diagnose hardware deviceinfo nic <port>”



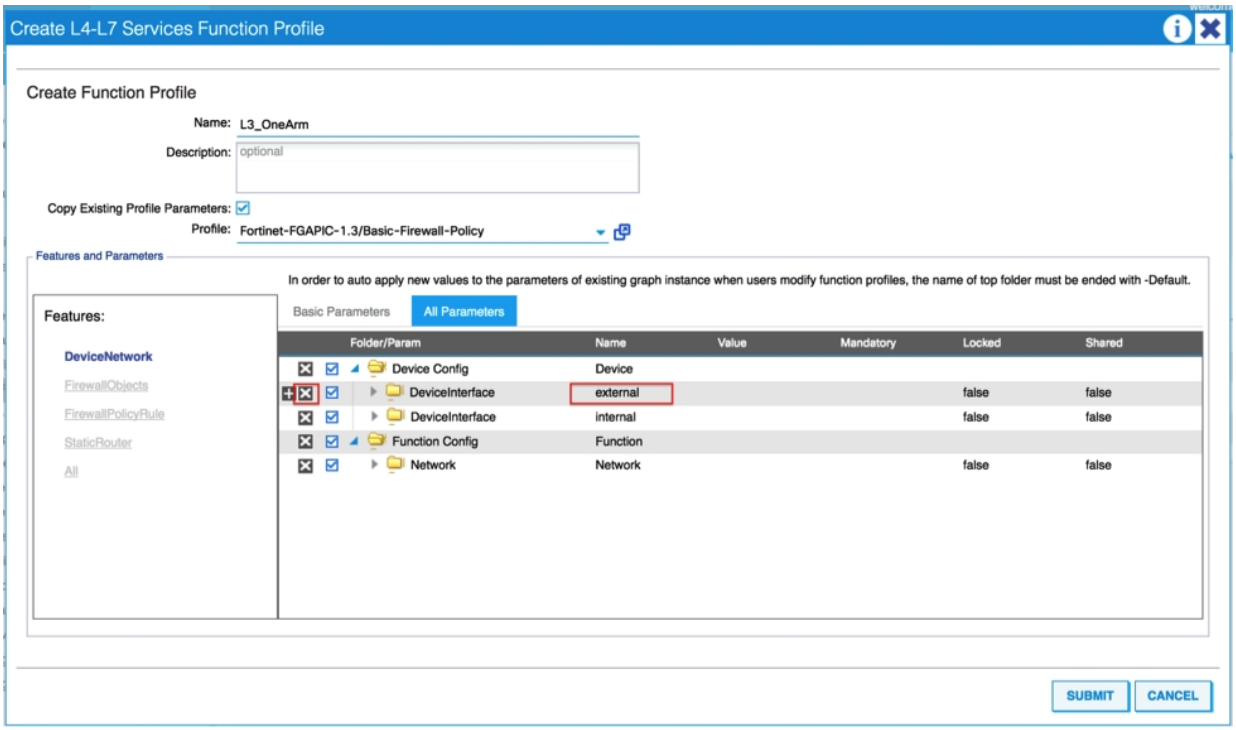
Create Device with Go-To mode with 2 logical interfaces on Cisco APIC (“internal” and “external”).

We will only utilize internal.



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation:

Device Config

Contains External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. We will delete the external interface since it is not utilized.

Function Config

Function Config consist of:

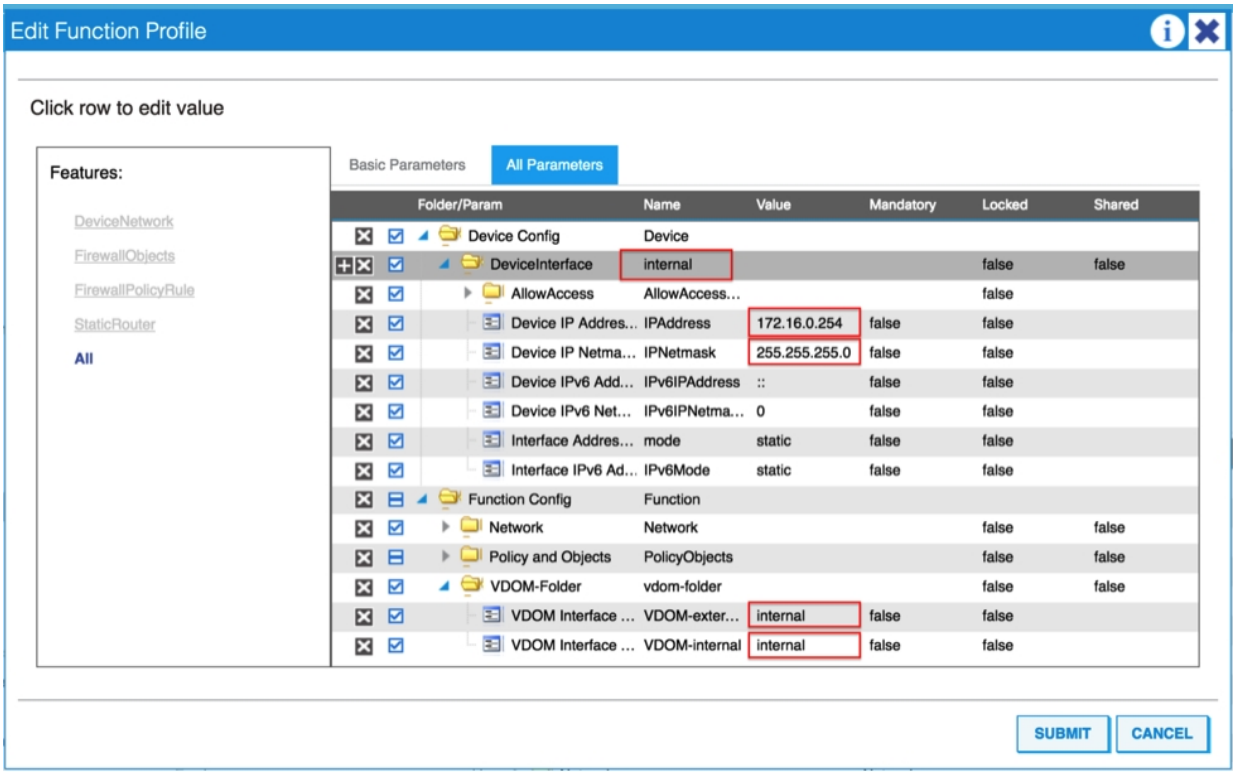
- Network
  - This field is use for configure Static Routes for IPv4 and IPv6.
- Policy and Objects

  This folder is the container for following list of folders:

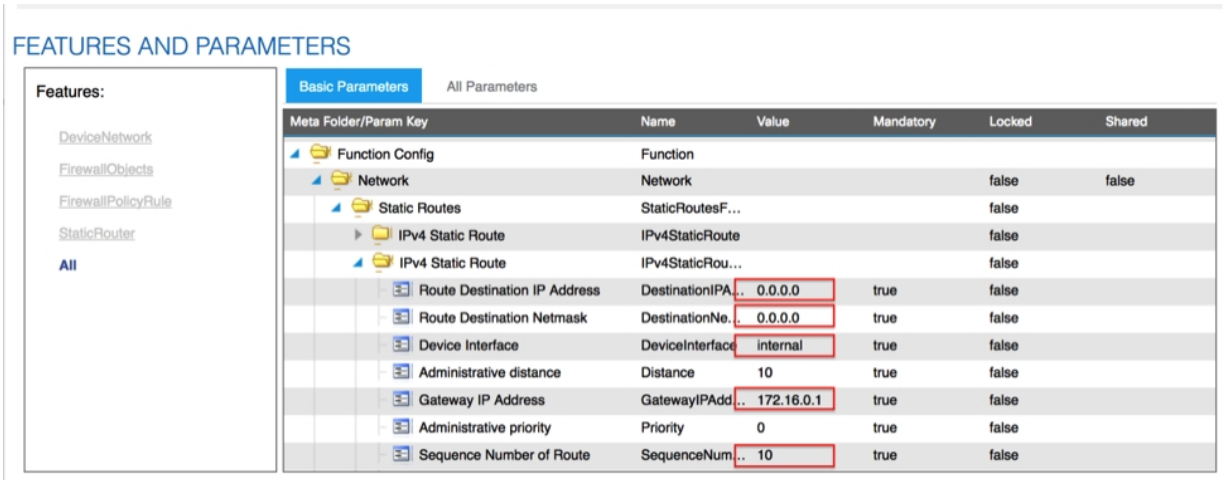
  - FWServiceFolder – Firewall Service Object container
  - IPv4/IPv6 DoS Policy – Dos Policy configuration
  - IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
  - IPv4 Policy – Firewall Policy Rule container
  - IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
  - ScheduleFolder – Schedule container

- VDOM-Folder
  - VDOM internal and external interfaces

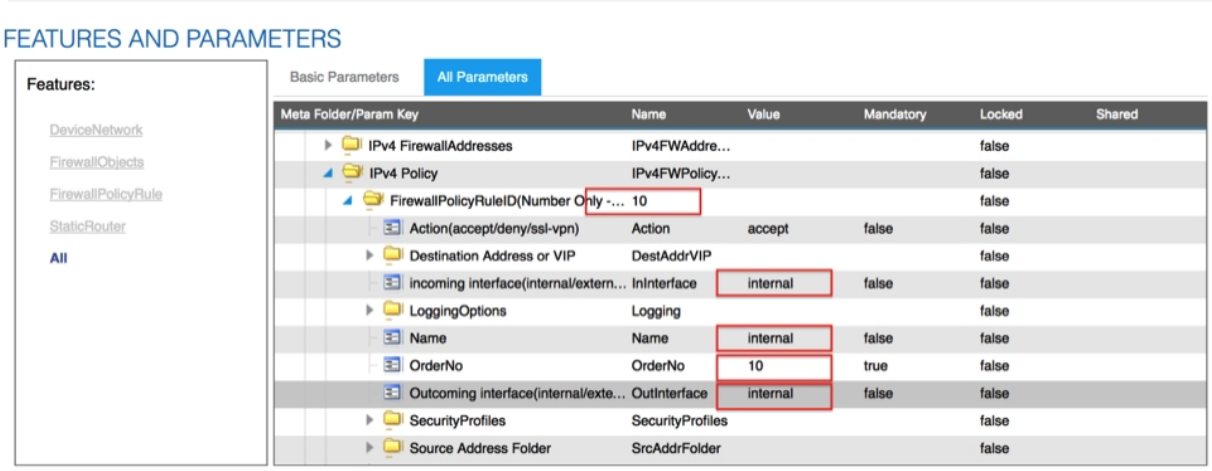
For this use case, internal is going to be shared for all service graph deployments. The Device IP Address will need to match the Policy Based Routing destination. Change the VDOM interfaces both to internal.



A single default route is needed and should point to the Dedicated Firewall Services BD Subnet IP Address.

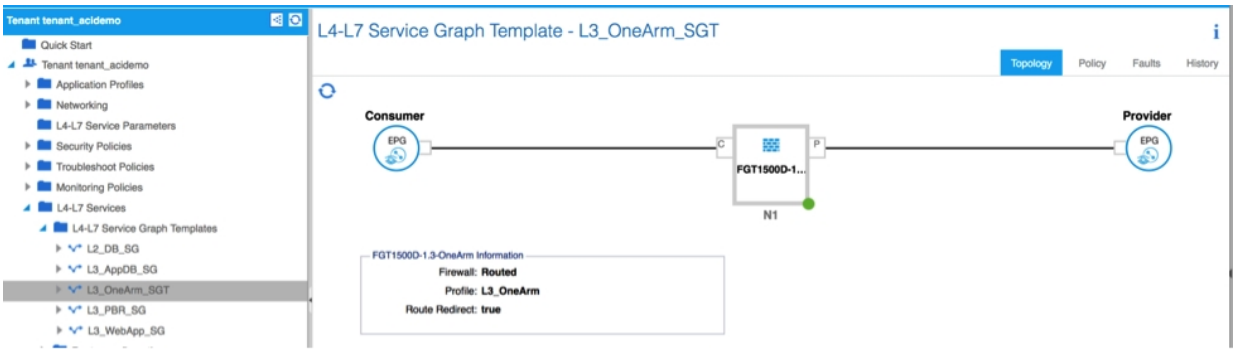


The Firewall Policies should utilize the same incoming and outgoing interfaces since this is a one-arm configuration.



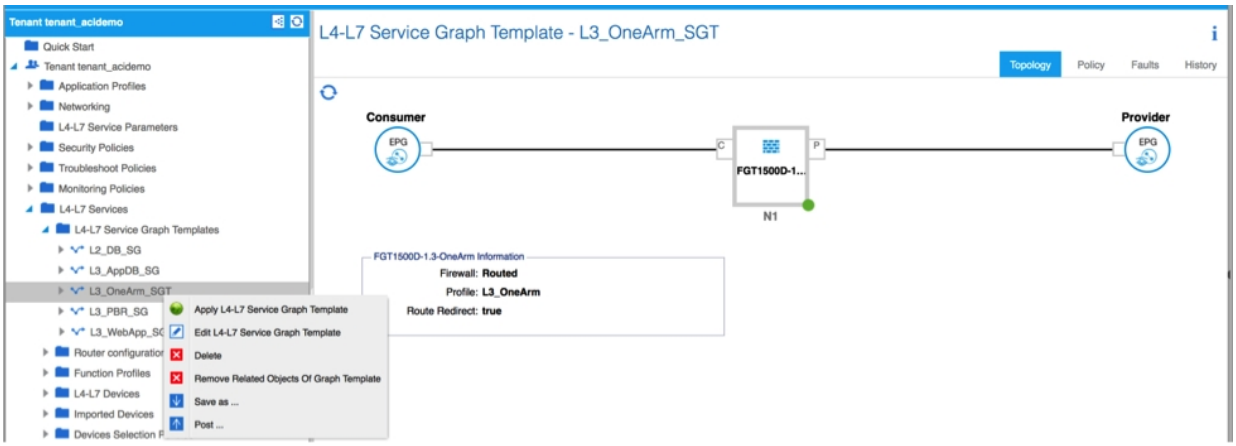
Create Service Graph1 for Web and App

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps. (Please check “Route Redirect” option box to enable Policy Based Routing)

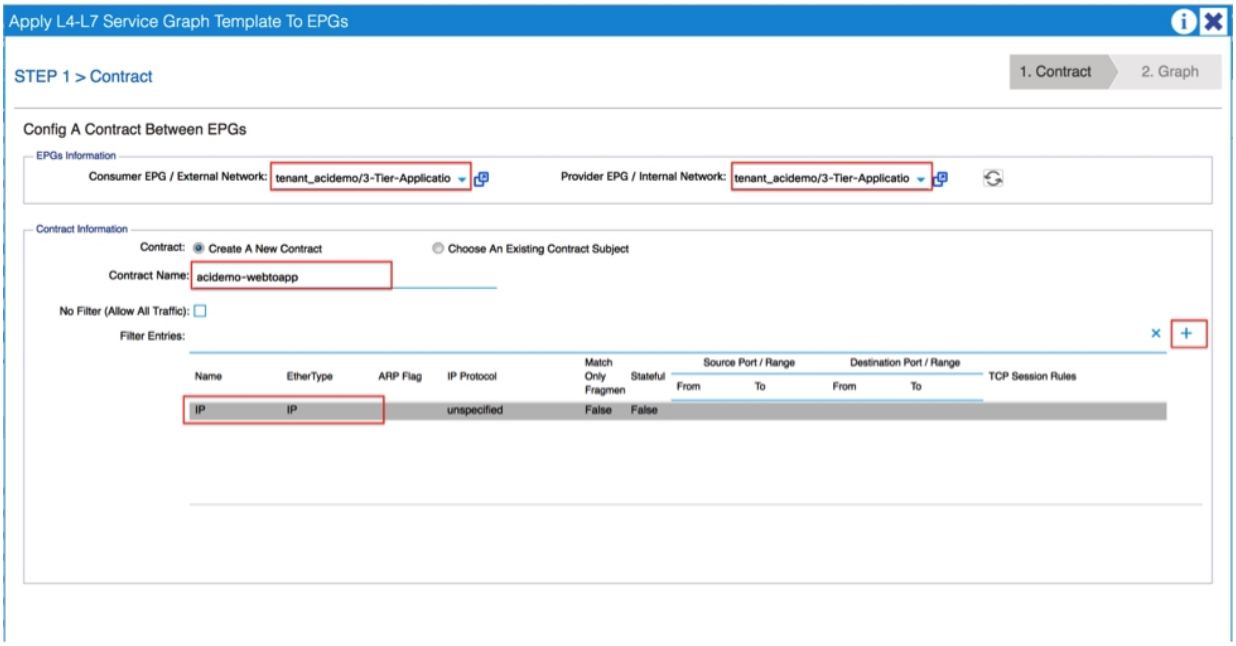


Deploy Service Graph1 Web to App

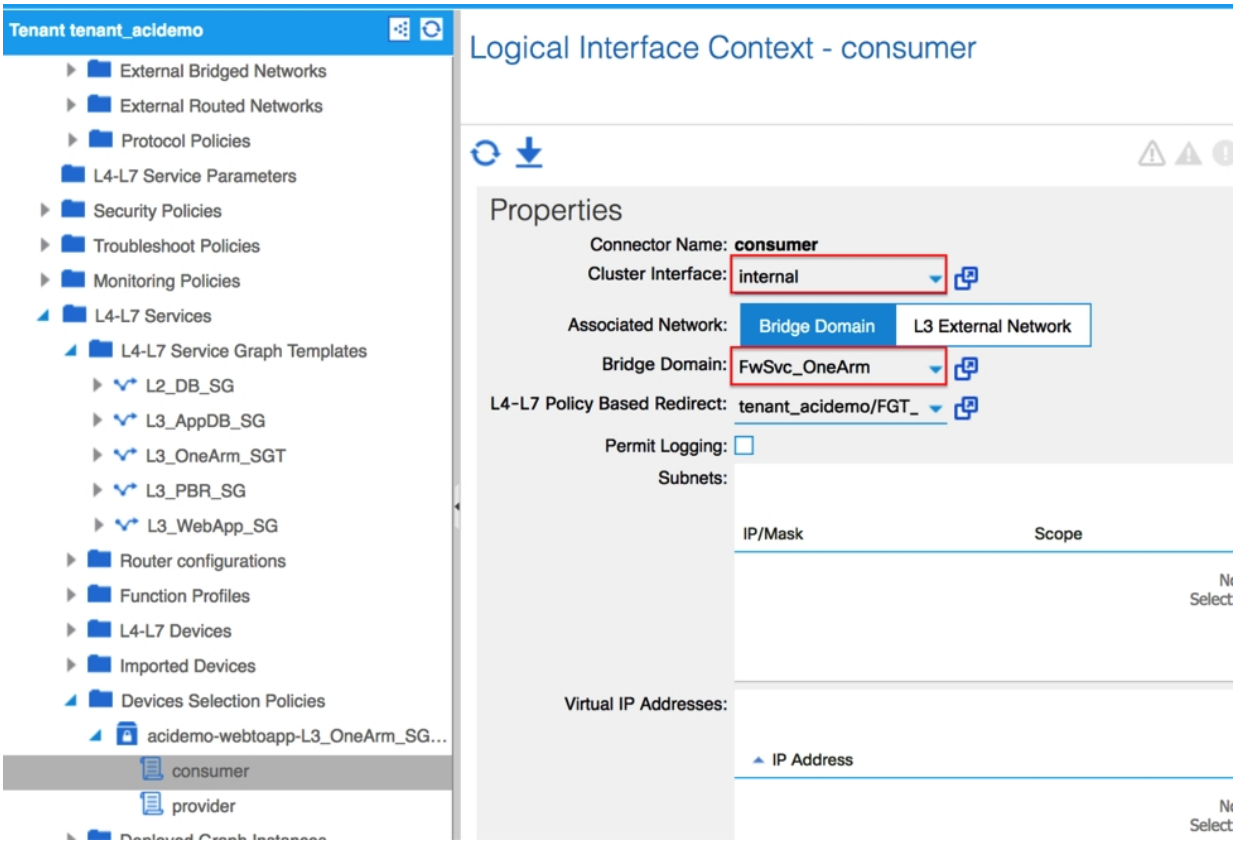
Once we combine the Firewall configuration and associated device together, we are ready to deploy Service Graph 1.



On next screen select the Consumer and provider EPGs (“Web” and “App”) and assign a contract name or select a pre-defined contract. For Policy Based Redirect, it is recommended to apply a filter and only redirect applicable traffic.

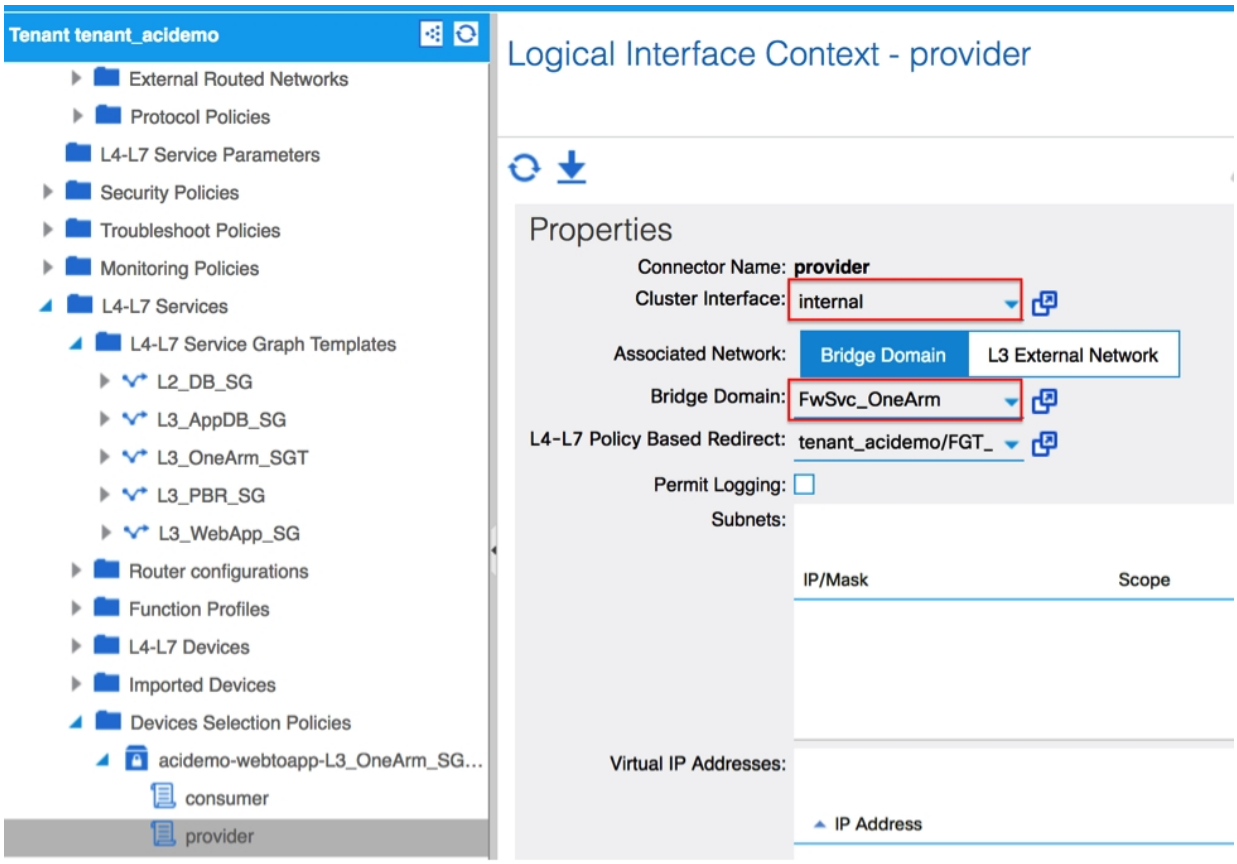


Next screen select the logical interfaces (“app” and “web”) defined during the creation of Layer4-7 Device.



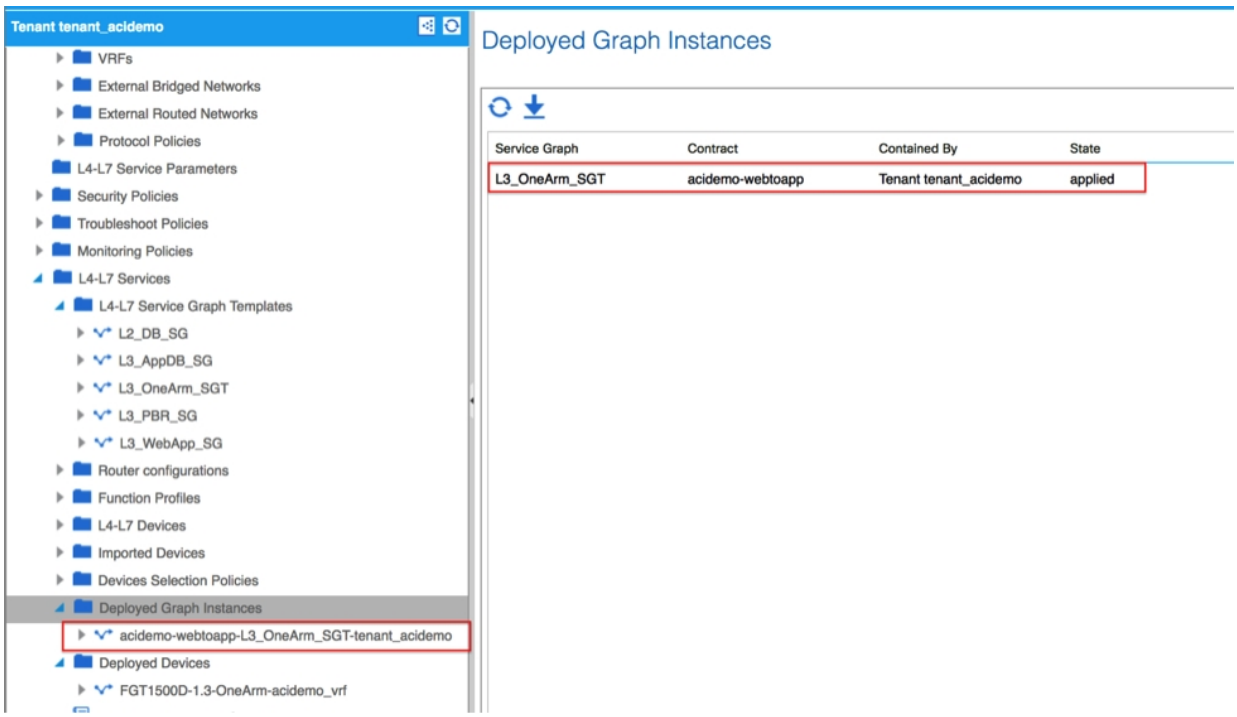
Due to an APIC GUI bug, it is necessary to select the incorrect BD now causing the SGT to fail to deploy. Select common/default, it will get remedied in the next steps.

Select the Device Selection Policy created by the previous step, consumer connector. Change to the correct BD, FwSvc_OneArm in our example. Make sure the cluster interface is set to internal.

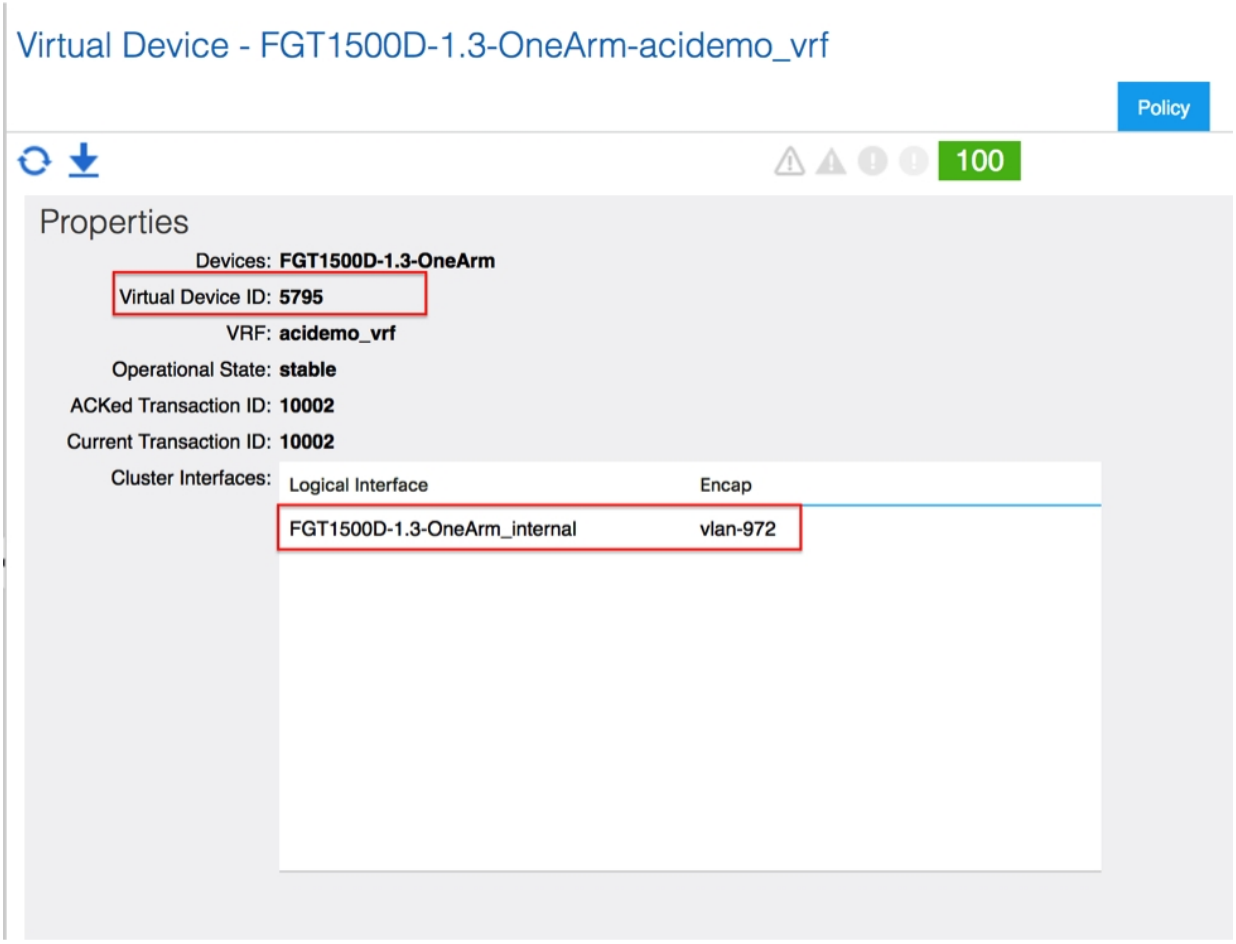


Now change the provider connector. Change the BD and cluster interface.

Verify Service Graphs Deployment



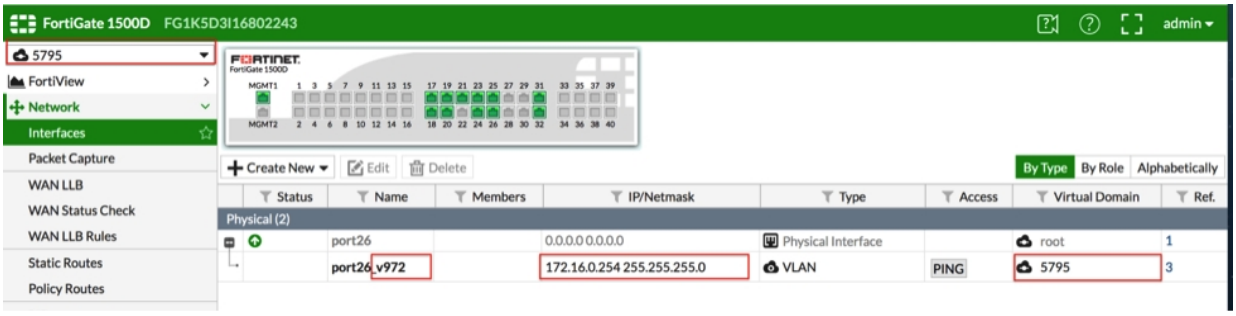
Verify Device Deployment



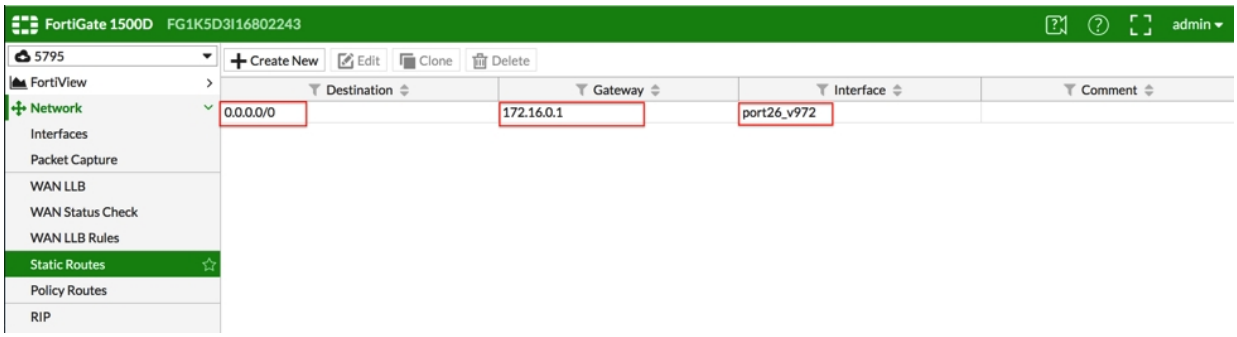
The Virtual Device ID is the VDOM ID which has been deployed to the Fortigate. The VLAN indicated has been applied to the interface created on the Fortigate under this VDOM for the internal interface.

Verify Fortigate Deployment

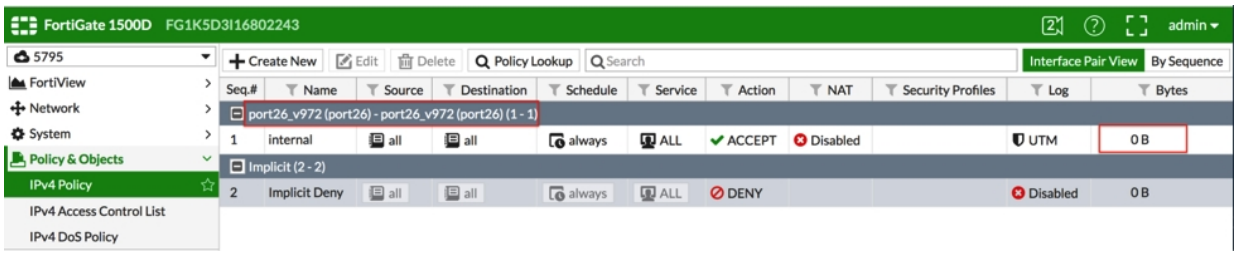
Verify the Network interface has been configured correctly.



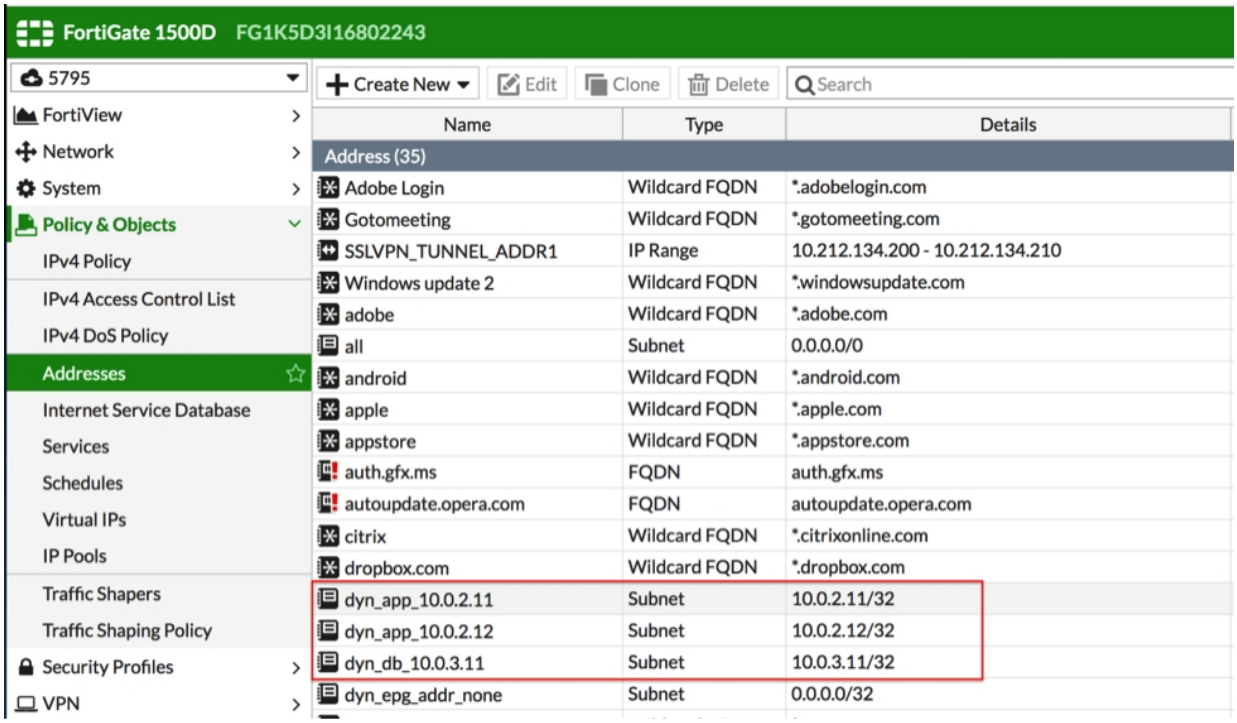
Verify the static route has been configured correctly.



Verify the Firewall Policy has been configured correctly. This policy shows traffic incoming and outgoing on same interface. No traffic has been seen yet matching this policy.



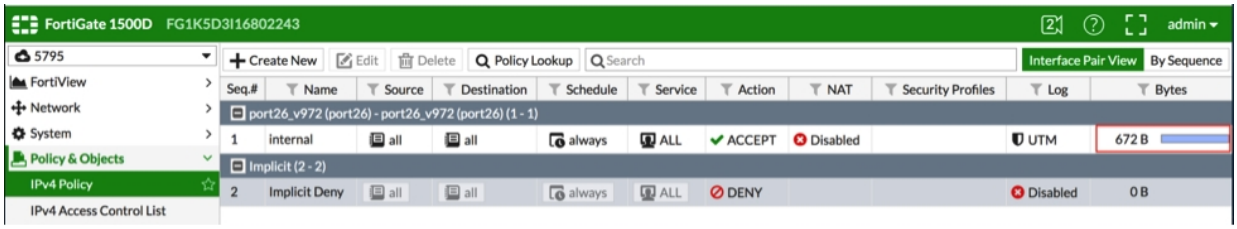
Verify the dynamic EPG address group has been updated.



Generate some traffic such as ping to verify connectivity.

```
root@App01:~# ping 10.0.3.11
PING 10.0.3.11 (10.0.3.11) 56(84) bytes of data.
64 bytes from 10.0.3.11: icmp_req=1 ttl=59 time=1.68 ms
64 bytes from 10.0.3.11: icmp_req=2 ttl=59 time=0.623 ms
64 bytes from 10.0.3.11: icmp_req=3 ttl=59 time=0.666 ms
64 bytes from 10.0.3.11: icmp_req=4 ttl=59 time=0.677 ms
^C
```

Check to see if the counters have increased.



APIC Infrastructure and FortiGate rollback

1. Upload and unload device package
2. Add and Delete device, FortiGate should clean-up previous configuration.
3. Dynamically modify and update policies
4. Detach and Attach service graphs
5. Delete tenants while service graphs in use.

Basic Troubleshooting

Verify Service Graph deployed

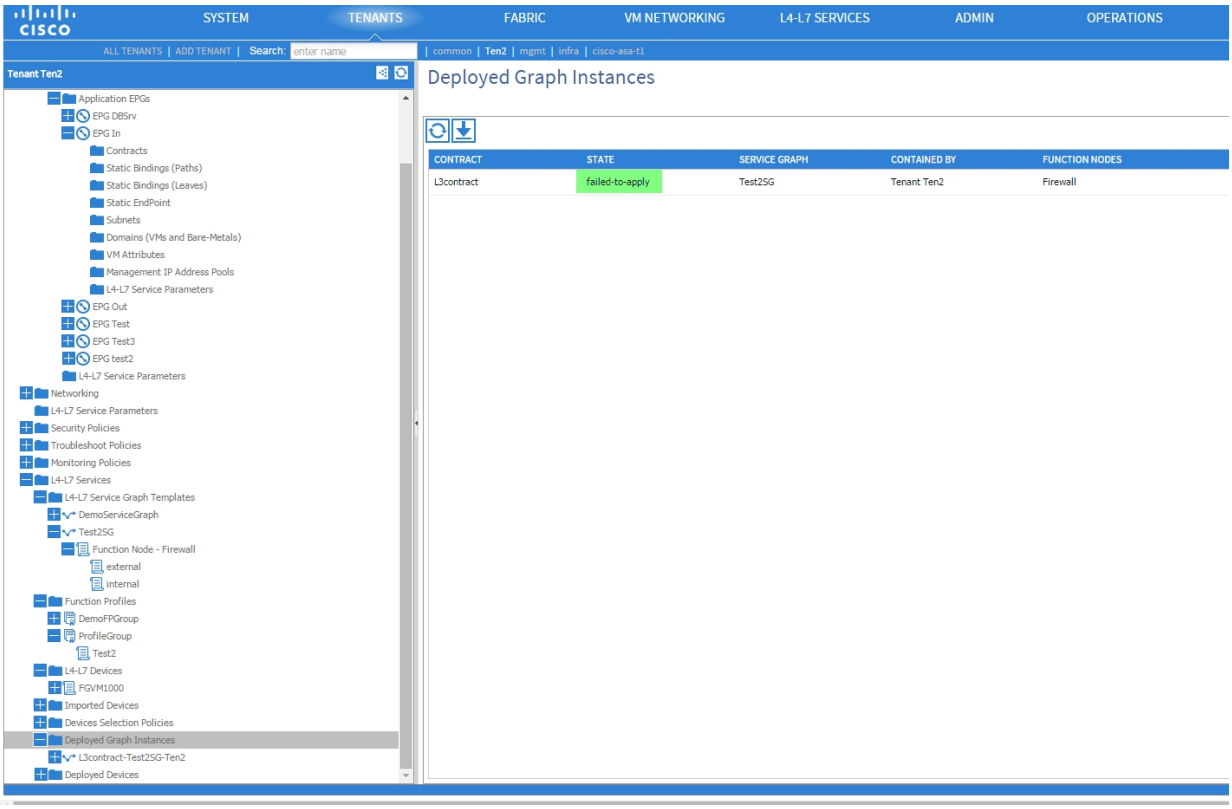
If Service Graph Deployed failed:

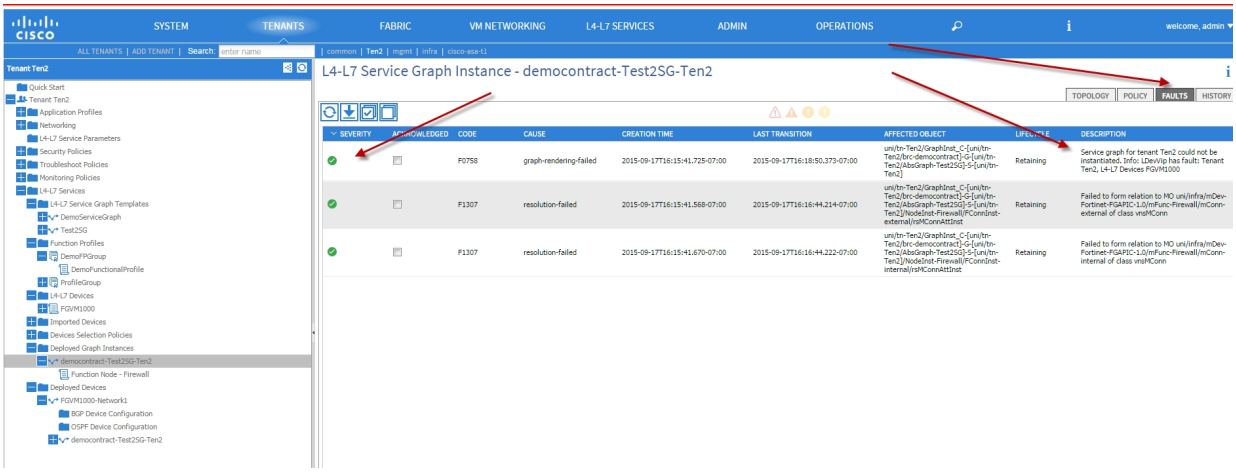
Navigate under ***Tenant > Deployed Graph Instances*** to check the state of the deployed graph.

If state is ***failed apply***, then go down one level to the ***Deployed Graph Instances*** and navigate to the ***Fault*** tab to check the error log. Any error code in 1000 range are relating to FortiGate while others belong to APIC

Currently we only have the following error code:

Error Code	Definition
1010	Configuration Error in device configuration
1020	Configuration Error in function configuration
1030	Internal Error -3
1040	Internal Error -4
1050	Internal Error -5
1070	Feature not available



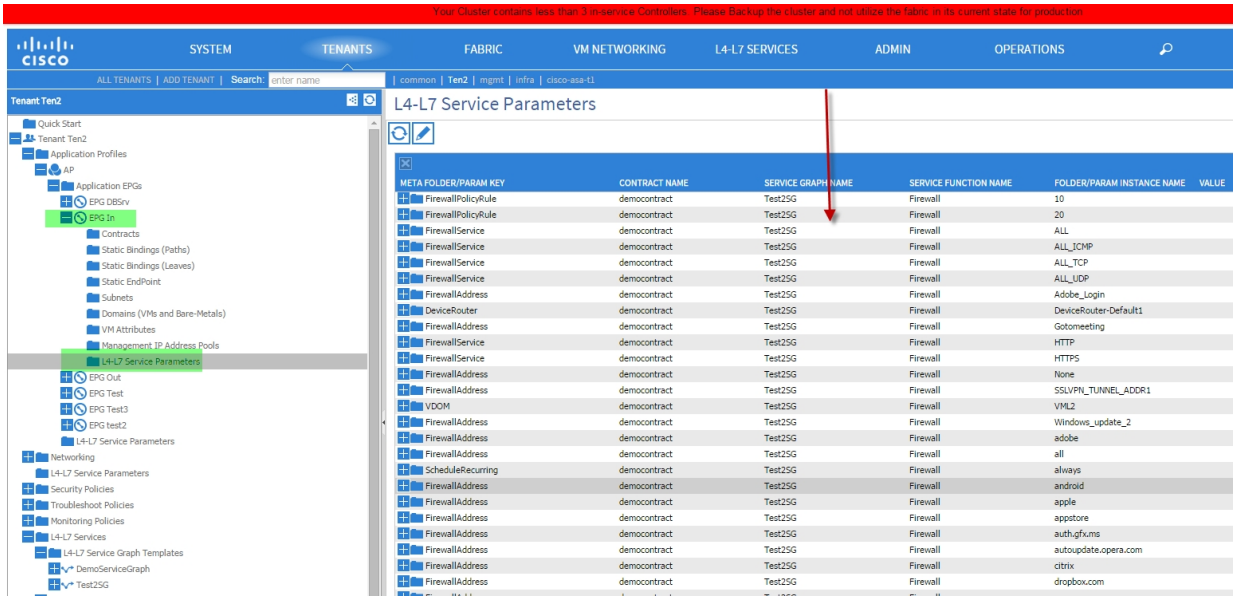


Service deployed but parameters missing

If Service deployed but certain parameters not showing up on Fortigate, please follow the below steps:

1. Navigate to ***Tenant> Provider EPG>L4-L7 Parameters***, ensure the missing parameters are listed.If not, double check the functional profile to confirm the configuration

Figure 1.



2. If yes, login on to Cisco APIC controller to examine the debug log. The debug log is located at `/data/devicescript/Fortinet.FGAPIC.1.3/logs` and the log file name is `debug.log`. Examine the log file and grab fields with "`[10.160.11.103, <xxxx>]:`" formats and scan through the logs associated to the parameters in question.
3. If all failed, please forward the entire captured log to Fortinet Technical Assistance Center for further troubleshooting.

FORTINET®

High Performance Network Security